LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturva-asetus poliisihallinnossa

Bergström, Samuli

2012 Turvallisuusosaamisen koulutusohjelma

Laurea-ammattikorkeakoulu
Turvallisuusosaamisen koulutusohjelma

Tietoturva-asetus poliisihallinnossa

Samuli Bergström
Turvallisuusosaamisen ko
Opinnäytetyö
Joulukuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusosaamisen koulutusohjelma

Tekijä(t)
Samuli Bergström

Tietoturva-asetus poliisihallinnossa

Vuosi 2012 Sivumäärä 70

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) astui voimaan 1.10.2010. Asetuksella on kolmen vuoden siirtymäaika perustason saavuttamiseksi ja viiden vuoden siirtymäaika korkeampien tasojen saavuttamiseksi. Asetus yhtenäistää valtionhallinnon salassa pidettävien tietoaineistojen luokittelun merkintöineen ja tuo konkreettisia vaatimuksia valtion virastojen tietoturvallisuuden hallitsemiseksi

Opinnäytetyö käsittelee kysymystä, kuinka valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa vaatimukset on otettu huomioon poliisin tietoturvallisuuden hallintajärjestelmässä ja jalkautetaan käytäntöön siirtymäaikojen puitteissa. Tavoitteena on kehittää malli tietoturva-asetuksen käyttöönotoksi poliisihallinnossa.

Poliisihallinnossa otettiin uusi luokitteluohjeistus käyttöön 1.1.2011 ja koulutettiin henkilöstölle pääsääntöisesti vuoden 2011 aikana. Poliisihallinnossa otettiin myös asetuksen määrittämät tietoturvatasot osaksi tietoturvallisuuden hallintajärjestelmää tammikuussa 2011. Tietoturvatasoihin perustuva toiminnan kehittäminen on parhaillaan kesken ja tähtää siirtymäaikojen puitteissa vaatimusten täyttämiseksi. Opinnäytetyössä kuvataan tietoturva-asetuksen käyttöönoton vuoksi tehdyt päätoimenpiteet poliisihallinnossa sekä keskeisiä kokemuksia joita tehdyistä toimenpiteistä on saatu. Lisäksi kuvataan palautteiden myötä mahdollisesti tehdyt keskeiset muutokset alkuperäiseen suunnitelmaan.

Tutkimuksessa selvisi, että pääsääntöisesti käyttöönotto on sujunut suunnitellusti ja poliisi on saavuttamassa tarvittavan tietoturvatason siirtymäajan vaatimassa aikataulussa. Tutkimuksessa havaittiin myös, että ohjeistuksen uusiminen ja sen jalkauttamiseksi järjestetyt turvallisuuskoulutukset ovat osaltaan parantaneet henkilöstön turvallisuustietoisuutta poliisissa.

Asiasanat: Tietoturvallisuus, tietojen luokittelu, tietoturvakoulutus

Laurea University of Applied Sciences **Abstract**
Leppävaara
Degree Programme in Security Competence

Name(s)
Samuli Bergström

Government Decree of Information Security at the Government at the police administration

Year 2012 Pages 70

Government Decree of Information Security at the Government (681/2010) was issued in 1.10.2010. The decree has 3 years transition time to achieve the basic level and 5 years transition time to achieve higher levels. The decree standardizes government information classification schema including markings and states concrete requirements for administering information security at the government bureaus.

This study addresses question, how the Government Decree of Information Security at the Government have been taken into account at the police information security management system and how it is implemented during the transition time. The goal is to develop a model to implement the Decree of Information Security at the police.

Police approved the new rules for information classification and handling 1.1.2011 and did train it to the employees during 2011. Police also adopted the government information security maturity system required by the decree as part of police information security management system in January 2011. The requirements issued by the adopted information security maturity system, is currently in progress and the aim is to comply the requirements during the transition time. This thesis describes the main actions that have been done at the police and also the main results that have issued from the actions including essential changes to the original implementation plan.

According to the study, implementation has mainly been passing as planned and the police will be achieving the required information security level at the required timeline. The study also showed that the results of updating the guidelines and especially the held trainings to help implement the new guidelines have improved the information security awareness at the police.

Keywords: Information security, information classification, information security awareness

Sisällys

1 Johdanto

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) astui voimaan 1.10.2010. Asetus määrittää kaksi keskeistä tietoturvallisuuden vaatimusta tai toimenpidettä valtionhallinnon virastoille. Karkeasti yksinkertaistettuna asetus pyrkii yhtenäistämään valtionhallinnon salassa pidettävien tietoaineistojen luokittelun merkintöineen ja tuo konkreettisia vaatimuksia valtion virastojen tietoturvallisuuden hallitsemiseksi.

Asetus tuo valtionhallinnon tietoturvallisuuden hallintaan kypsyystasoajattelun, jonka mukaan virastossa käsiteltävä tiedon suojaustaso määrittää kuinka kyvykästä tietoturvallisuuden hallinta tulee olla. Asetuksella on kolmen vuoden siirtymäaika perustason saavuttamiseksi ja viiden vuoden siirtymäaika korkeampien tasojen saavuttamiseksi.

Tämä opinnäytetyö käsittelee kysymystä, kuinka valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (myöhemmin tietoturva-asetus) vaatimukset on otettu huomioon poliisin tietoturvallisuuden hallintajärjestelmässä ja jalkautetaan käytäntöön siirtymäaikojen puitteissa.

Tämän opinnäytetyön tavoitteena on kehittää malli tietoturva-asetuksen käyttöönotoksi poliisihallinnossa.

Opinnäytetyön ulkopuolelle rajataan asiaan liittyvät salassa pidettävät suunnitelmat ja selvitykset. Opinnäytetyön ulkopuolelle rajataan myös lain kansainvälisistä turvallisuusvelvoitteista (588/2004) tai kansainväliseen tiedonvaihtoon liittyvien asiakirjojen hallinta tai hallinnan kehittäminen poliisihallinnossa.

2 Tietoturvallisuus poliisihallinnossa

Sisäasiainministeriön poliisiosasto vastaa poliisin toimialan ohjauksesta ja valvonnasta. Sisäasiainministeriön alainen Poliisihallitus johtaa ja ohjaa operatiivista poliisitoimintaa toimien poliisin keskushallintoviranomaisena. Poliisihallituksen alaisuudessa toimivat poliisin valtakunnalliset yksiköt keskusrikospoliisi, suojelupoliisi, liikkuva poliisi, poliisiammattikorkeakoulu sekä poliisin tekniikkakeskus ja poliisin 24 poliisilaitosta. Poliisihallinto on noin 11000 henkilön organisaatio, joista poliiseja on noin 7700 henkilöä (Poliisin vuosikertomus 2011).

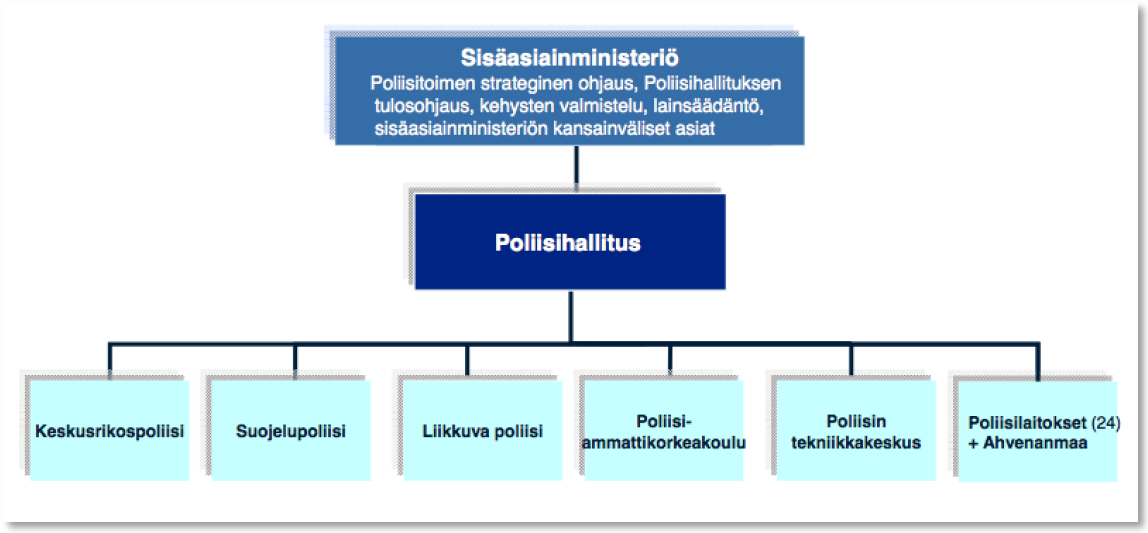
Tietoturvallisuus poliisissa on osa poliisin organisaatioturvallisuutta joka on sijoitettu Poliisihallituksen esikuntayksikköön. Poliisin tietoturvallisuutta johtaa poliisiylijohtaja. Poliisin tietoturvapäällikkö vastaa poliisihallinnon tietoturvallisuuden ja tietosuojan ohjaamisesta, valvonnasta, kehittämisestä ja yhteensovittamisesta sekä poliisin ylimmän johdon raportoinnista. (Poliisin tietoturvapolitiikka 2010.)

Poliisin yksiköiden johto vastaa yksikön tietoturvallisuudesta ja tietoturvatyön johtaminen on osa normaalia johtamis- sekä tulosohjausprosessia. Jokaisessa poliisin yksikössä on nimetty tietoturvapäällikkö tai –vastaava. Mikäli tietoturvapäällikköä tai –vastaavaa ei nimetä, tehtävää hoitaa yksikön turvallisuuspäällikkö. Yksikön tietoturvapäällikön tai –vastaavan tehtävänä on:

- valvoa ja tarkastaa säännöllisesti yksikön tietoturvallisuuden tilaa;
- koordinoida, kehittää ja ylläpitää yksikön tietoturvallisuutta;
- kouluttaa ja ohjata turvallisia toimintatapoja yksikössä;
- vastata tietoturvallisuuden poikkeustilanteisiin reagoinnista yksikön osalta sekä
- ylläpitää tietoturvallisuuden tilannekuvaa ja
- raportoida tietoturvallisuudesta yksikön johdolle sekä poliisin tietoturvapäällikölle.

(Poliisin tietoturvapolitiikka 2010.)

Turvallisuushenkilöstö on muutamaa poikkeusta lukuun ottamatta osa-aikaisia ja henkilöiden mahdollisuus käyttää aikaa turvallisuustehtäviin vaihtelee huomattavasti yksiköittäin. Turvallisuushenkilöstö on sijoitettu poliisihallinnossa pääsääntöisesti tehtävistä riippuen päällystöön tai alipäällystöön.



Kuva 1: Poliisin hallintorakenne (Poliisin hallintorakenne 2012.)

3 Tutkimusaiheeseen liittyvää keskeistä säännöstöä

3.1 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa tuli voimaan 1.10.2010 valtioneuvoston päätöksellä ja oikeusministeriön esittelystä. Tietoturva-asetus täydentää vuodelta 1999 voimassa olevaa lakia viranomaisen toiminnan julkisuudesta (621/1999, myöhemmin Julkisuuslaki).

Tietoturva-asetus kumoaa osittain asetuksen viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999, myöhemmin Julkisuusasetus). Kumotut kohdat koskevat erityissuojattavan tiedon luokitteluja ja käsittelyä koskevia pykäliä jotka määritetään tarkemmin tietoturva-asetuksessa.

Tietoturva-asetus koostuu viidestä luvusta

1. Yleiset säännökset
2. Yleiset tietoturvallisuusvaatimukset
3. Asiakirjojen luokittelu
4. Luokitellun asiakirjan käsittelyä koskevat vaatimukset
5. Voimaantulo

(Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 2010.)

3.1.1 Yleiset säännökset

Tietoturva-asetuksen ensimmäisessä luvussa kuvataan soveltamisala, suhde muuhun lainsäädäntöön sekä määritelmät. Asetuksen soveltamisalaksi määritetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevat yleiset tietoturvavaatimukset sekä luokittelun perusteet ja käsittelyssä noudatettavat tietoturvavaatimukset. Toisin sanoen asetus määrittää poliisihallinnolle yleisiä, organisaatiota koskevia tietoturvavaatimuksia sekä vaatimuksia yksittäisen asiakirjan käsittelyyn.

3.1.2 Yleiset tietoturvallisuusvaatimukset

Asetuksen toisessa luvussa kuvataan virastolle asetettavat yleiset vaatimukset tietoturvallisuuden perustason toteuttamiseksi. Luvussa määritetään että tietoturvallisuus tulee olla suunnitelmallista, hyvän tiedonhallintatavan mukaista ja että se tulee mitoittaa käsiteltävien asiakirjojen merkityksen mukaisesti. Asiakirjojen käsittelyn turvaamisessa on otettava huomioon koko tiedon elinkaari. Suunnittelussa on otettava huomioon myös turvallisuustoimenpiteistä aiheutuvat kustannukset.

Tietoturvallisuuden perustason toteuttamiseksi on määritetty 10 vaatimusta jotka tulee täyttää riippumatta käsitteleekö viranomainen salassa pidettäväksi luokiteltavaa tietoa.

1. viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan;
2. viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3. asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4. tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5. asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6. tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7. asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8. henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;

9. henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10. annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

(Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 2010.)

Asetuksen toisen luvun 7 § kuvaa mahdollisuuden asiakirjojen luokittelupäätöksen tekemisestä virastossa. Mikäli viranomainen päättää luokitella tietonsa, tulee se tehdä asetuksen luvun 3 vaatimusten mukaisesti ja asiakirjojen käsittelyssä tulee noudattaa luvun 4 vaatimuksia. Huomioitavaa luvussa on että siinä ei oteta kantaa tilanteeseen, jossa viranomainen on jo ennen asetuksen voimaan tuloa tehnyt päätöksen luokittelun käyttöönotosta. Näinhän on toimittu esimerkiksi useimpien turvallisuusviranomaisten, kuten poliisin osalta aiemmin voimassa olleen julkisuusasetuksen 2 § ja 3 § mukaisesti.

3.1.3 Asiakirjojen luokittelu

Tietoturva-asetuksen kolmas luku määrittää luokittelun ja salassa pidettävien asiakirjojen merkitsemisen perusteet, mikäli viranomainen on 7 § mukaisesti tehnyt päätöksen luokittelusta. Asetuksen mukaan luokittelu voidaan tehdä myös osittaisena, eli kohdistaa luokittelu vain asiakirjoihin tai niiden käsittelyvaiheisiin joissa luokittelua tarvitaan.

Luokittelua voidaan käyttää ainoastaan lain perusteella salassa pidettäviin asiakirjoihin. Julkisuuslaki määrittää keskeiset salassa pidon perusteet, mutta myös muussa lainsäädännössä asetetaan asiakirjojen tai tietojen salassapitoon ja käytön rajoittamiseen liittyviä säädöksiä.

Julkisuusasetus määritti aiemmin luokittelun kolmiportaiseksi, tietoturva-asetus tuo mukanaan neljä luokkaa joita kutsutaan suojaustasoiksi. Asiakirja tai tieto luokitellaan eri suojaustasolle oikeudettomasta paljastumisesta tai käytöstä arvioidun haitan perusteella.

1. suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
2. suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
3. suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;

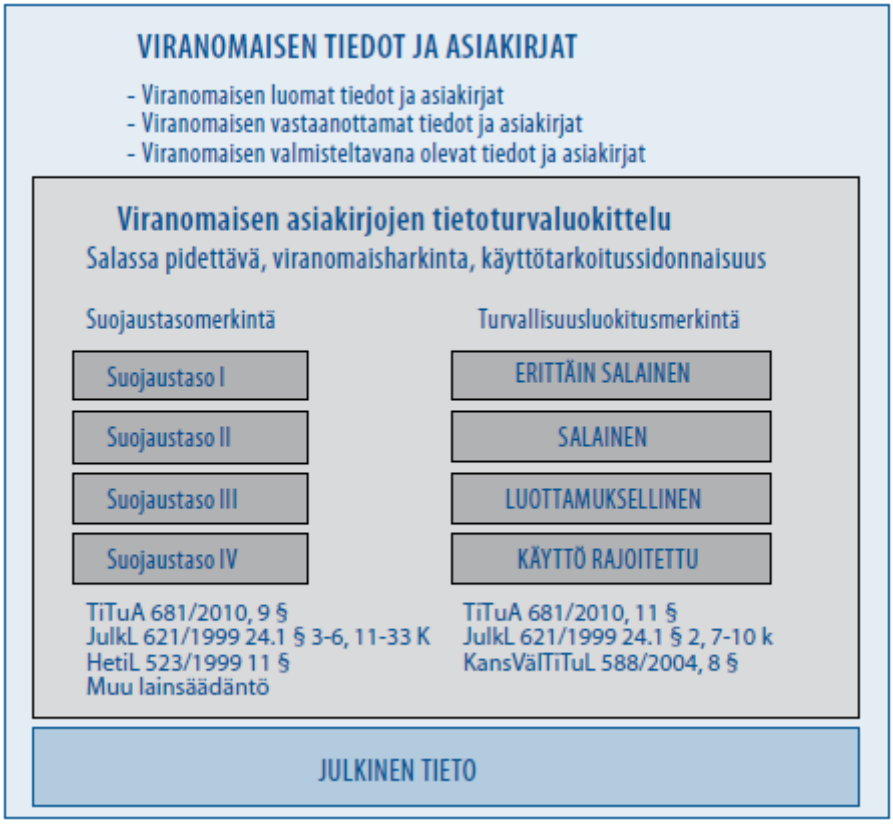
4. suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle

(Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 2010.)

Edellä mainittujen perusteiden lisäksi suojaustasolle IV voidaan luokitella asiakirja viranomaisen harkinnan tai käyttötarkoituksen perusteella.

Asetuksen kolmannen luvun 10 § kuvaa luokitusmerkintöjen tekemistä asiakirjoihin. Merkintä voidaan tehdä Julkisuuslain 25 § mukaisesti eikä toisen viranomaisen tekemää merkintää saa muuttaa ilmoittamatta viranomaiselle (pois lukien suojaustason IV asiakirjat). Valtiovarainministeriön ohje tietoturvallisuudesta annetun asetuksen täytäntöönpanosta (myöhemmin VAHTI 2/2010) ohjeistaa merkintöjen tekemisestä tarkemmalla tasolla.

Neljä erilaista suojaustasoa jaetaan vielä kahteen riippuen salassapidon perusteesta. Salassapidon perusteella osa asiakirjoista turvallisuusluokitellaan ja osa merkitään salassa pidettäväksi määritetylle suojaustasolle ilman turvallisuusluokittelua.



Kuva 2: Viranomaisen tietojen luokittelu (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 31.)

Asiakirja tai tieto voidaan lisäksi turvallisuusluokitella muutamalla perusteella (kuva 2). Käytännössä perusteet koskevat Suomen kansainvälisiä suhteita, maanpuolustusta, suojelupoliisin toimintaa, varautumista poikkeusoloihin sekä viranomaisen turvallisuusjärjestelmiä. Turvallisuusluokitusta ei saa ulottaa asetuksen perusteita laajemmalle.

3.1.4 Luokitellun asiakirjan käsittelyä koskevat vaatimukset

Asetuksen neljäs luku kuvaa yleisellä tasolla eri suojaustasoille määritetyt käsittelyvaatimukset. Käsittelyvaatimuksia tarkennetaan huomattavasti Valtiovarainministeriön ohjeessa tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010).

Suojaustasoilla I-III sekä suojaustasolla IV koskien arkaluonteisia henkilötietoja ja biometrisiä tunnistetietoja tallennettuna henkilörekisteriin, tulee käyttöoikeuden perustua työtehtävien mukaiseen tarpeeseen. Työtehtävistä on pidettävä luetteloa suojaustasoilla I ja II sekä tietyin rajauksin suojaustasoilla III ja IV. Asetus viittaa myös henkilöstön luotettavuuden arviointiin, joista säädetään muualla.

Luvun neljä 14 § ja 15 § määrittävät vaatimuksia fyysiseen käsittelyyn. Keskeistä pykälissä on että tilat ja asiakirjat ovat asianmukaisesti lukittuja, tiloissa liikkuvat henkilöt tunnistetaan ja rajoitetaan asiakirjojen käsittelyä toimitilojen ulkopuolella.

3.2 Muu asiaan keskeisesti liittyvä lainsäädäntö ja ohjeistus

3.2.1 Laki viranomaisen toiminnan julkisuudesta

Laki viranomaisen toiminnan julkisuudesta (Julkisuuslaki) määrittää perusteet viranomaisen toiminnan ja asiakirjojen julkisuudesta ja salassa pidosta. Luvussa 3.1 kuvattu tietoturva-asetus täydentää tätä lakia. Laki on tullut voimaan 21.5.1999.

Lain keskeisin periaate on, että ”Viranomaisen asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä” (Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta 1999). Laki määrittää myös perusteet sille, missä julkisuuslakia sovelletaan, mikä on viranomaisen asiakirja ja mitä velvollisuuksia viranomaisella on tiedonsaantia ja hyvää tiedonhallintatapaa koskien.

3.2.2 Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (Julkisuusasetus) tuli alkuperäisenä voimaan 12.11.1999 täydentämään aiemmin kuvattua julkisuuslakia.

Asetuksessa tarkennetaan eräitä julkisuuslain käsitteitä ja määritelmiä. Tietoturva-asetus korvasi voimaan tullessaan 1.10.2010 asetuksen 2 ja 3 § jotka kuvasivat aiemmin erityissuojattavien tietoaineistojen käsittelyvaatimuksia.
(Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1999.)

3.2.3 Valtiovarainministeriön ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta

Valtiovarainministeriö julkaisi 16.10.2010 ohjeen tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010). Ohjeen tavoitteena on saatesanojen mukaan ”tehostaa ja yhdenmukaistaa lain viranomaisen toiminnan julkisuudesta (621/1999) perusteella 1.7.2010 annetun ja 1.10.2010 voimaantulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanoa”. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 5.)

Lähes sataviisikymmentäsivuinen ohje tarkentaa asetuksen vaatimuksia huomattavasti. Ohje käsittää tarkan kuvauksen vaatimuksista miten tietoaineistot tulee luokitella ja käsitellä, sekä toimenpiteistä jotka viranomaisen on toteutettava saavuttaakseen tarvittavan tietoturvallisuuden kyvykkyyden.

Ohje tuo valtionhallintoon käsitteenä tiedon suojauksen tarpeeseen perustuvat konkreettiset vaatimukset jotka lisääntyvät suojaustarpeen kasvaessa (tietoturvatasot). Ohje sisältää sekä hallinnollisia että teknisiä vaatimuksia. Ohjeen sisältö on kuvattu karkealla tasolla alla olevassa taulukossa (taulukko 1).

Luku	**Keskeinen sisältö**
1 Johdanto	Kuvaa ohjeen tarkoituksen ja soveltamisalan, avaa keskeiset käsitteet ja aihetta koskevan regulaation.
2 Asetuksen täytäntöönpanosta	Kuvaa asetuksen täytäntöönpanon keskeiset edellytykset.
3 Hyvä tiedonhallinta- ja tiedonkäsittelytapa	Tarkentaa hyvän tiedonhallintatavan ja tiedon käsittelytavan vaatimuksia ja avaa siihen liittyvää regulaatiota.
4 Tietojenkäsittelyn yleiset tietoturvavaatimukset	Kuvaa tietojenkäsittelyn yleisiä vaatimuksia, kuten luokittelua, henkilöstöä, tietoturvakulttuuria ja tilaturvallisuutta koskevia edellytyksiä.
5 Tietoteknistä ympäristöä koskevia tietoturvavaatimuksia	Kuvaa tietoteknistä ympäristöä koskevat vaatimukset ja esittelee tietojärjestelmiin liitettävät tietoturvallisuustasot.

6 Hallinnollista tietoturvallisuutta koskevia vaatimuksia	Määrittää tietoturvatasojen sisällön, kuvataan tarkemmin ohjeen liitteessä 5.
7 Tietoaineistojen luokittelu	Kuvaa tietoaineistojen luokittelun periaatteet.
8 Luokiteltujen tietoaineistojen käsittelyvaatimuksia	Kuvaa salassa pidettävien tietoaineistojen käsittelyvaatimukset.
Liitteet	Liite 1 listaa voimassa olevan regulaation Liite 2 kuvaa sallitut salassapitoleimat Liite 3 kuvaa ohjeita ja vaatimuksia asiakirjojen käsittelyn mahdollistamiseksi viranomaisessa Liite 4 kuvaa salassa pidettävien asiakirjojen käsittelyvaatimukset tiedon eri elinkaaren vaiheissa Liite 5 kuvaa tietoturvatasojen yksityiskohtaiset vaatimukset Liite 6 kuvaa korvaavan menettelyn mikäli vaatimuksia ei voida tai ole järkevää täyttää Liite 7 listaa voimassa olevat VAHTI julkaisut

Taulukko 1; VAHTI 2/2010 Keskeinen sisältö (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 11-12.)

Ohjeen eräs keskeisimpiä asioita on tietoturvatasojen yksityiskohtaiset vaatimukset ohjeen liitteessä 5. CAF -laatumallista johdetut tietoturvatasovaatimukset jaetaan hallinnollisiin ja tietojärjestelmiin kohdistuviin vaatimuksiin. Alla on kuvattu tietoturvatasojen pääotsikot.

- Tietoturvallisuuden hallinnan vaatimukset
    - Johtajuus
    - Strategiat ja toiminnan suunnittelu
    - Henkilöstö
    - Kumppanuudet ja resurssit
    - Toiminnan prosessit
    - Mittaaminen

- Tietojärjestelmien hallinnan vaatimukset
    - Raportointimenettelyt
    - Omaisuuden hallinta
    - Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto
    - Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta
    - Turva-alueiden muodostus ja niiden välinen suodatus
    - Pääsynvalvonta
    - Käyttäjien ja käyttövaltuuksien hallinta

- Haittaohjelmilta suojautuminen
- Fyysisen ympäristön suojaaminen
- Varmuuskopiointi
- Tietoturvallisuutta vaarantavien poikkeamien valvonta
- Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta

Kukin pääotsikko jakautuu vielä yhteen tai useampaan alaotsikkoon ja niistä eri tietoturvatasoille määrittyviin vaatimuksiin (kuva 3). Korkeamman tason tietoturvavaatimukset tulevat alempien lisäksi.
(Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 45-48.)

2.1 Raportointi tietoturvavastaavalle

Osa-alueen nimi	2.1 Raportointi tietoturvavastaavalle
Tavoitteet	Tietoturvavastaava saa tietoa tietoturvallisuuden tilasta johdolle raportointia sekä tietoturvamekanismien ja -prosessien riittävyyden ja vaikuttavuuden arviointia varten.
Perustason vaatimukset	1. Säännöllinen raportointi IT-järjestelmien ja niiden hallinnan tietoturvallisuuden tilasta tietoturvavastaavalle on organisoitu ja vastuutettu. 2. Vakavista tietoturvatapahtumista kerrotaan tietoturvavastaavalle viivytyksettä.
Korotetun tason lisävaatimukset	3. Raportointi on kirjallinen.
Korkean tason lisävaatimukset	4. Raportointi perustuu sovittuihin tietoturvatavoitteisiin ja niiden mittareihin.
Käytännön esimerkkejä	• Vaatimukseen 1: Tietoturvapäällikkö käy joka kuukausi palaverissa tietohallinnon kanssa, jolloin käsitellään tehtyjä tietoturvallisuuden kehitystoimia, päivityksiä ja uusia havaittuja uhkia ja riskejä. • Vaatimukseen 1: Organisaatio on ulkoistanut IT-järjestelmien ylläpitoa kahdelle eri alihankkijalle. Palvelutasosopimuksissa lukee, miten alihankkija raportoi tietoturvatilanteesta palveluvastaavalle. Palveluvastaava raportoi edelleen tietoturvapäällikölle.
Apuvälineitä ja malleja	Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006) • Luku 5.6: Esimerkki raportointimenettelyistä ja raportin sisällöstä
Huomioita	Tiedon tulee kulkea käytännön tasolta ylöspäin. Perustasolla riittää suullinen raportointi, sähköposti tai muut kirjalliset keinot ovat kuitenkin parempia.

Kuva 3: Esimerkki VAHTI 2/2010 tietoturvatasojen vaatimuksista (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 113.)

4 Kehittämisprosessi ja sen rajoitteet

4.1 Toimintatutkimus kehittämismenetelmänä

Tässä kehittämistyössä käytetään menetelmänä toimintatutkimuksen mallia. ”Toimintatutkimus on yleisnimitys sellaisille lähestymistavoille, joissa tutkimuskohteeseen pyritään tavalla tai toisella vaikuttamaan, tekemään tutkimuksellisin keinoin käytäntöön kohdistuva interventio.” (Eskola & Suoranta 2005, 126).

Toimintatutkimus on lähestymistapa, jossa tutkija osallistumalla kiinteästi tutkittavana olevan kohteen elämään pyrkii yhdessä sen jäsenten kanssa ratkaisemaan jotkin ratkaistaviksi aiotut ongelmat, saavuttamaan yhdessä kohteen jäsenten kanssa asetetut tavoitteet ja päämäärät, tutkimalla näiden ongelmien ilmenemistä, synty- ja kehitysehtoja ja niiden ratkaisuun johtavia teitä toimimalla saadun tiedon ja kehitettyjen ratkaisuvaihtoehtojen pohjalta yhdessä kohteen jäsenten kanssa ongelmien ratkaisemiseksi, tavoitteiden saavuttamiseksi, päämääriin pääsemiseksi. (Jyrkämä 1978, 39).

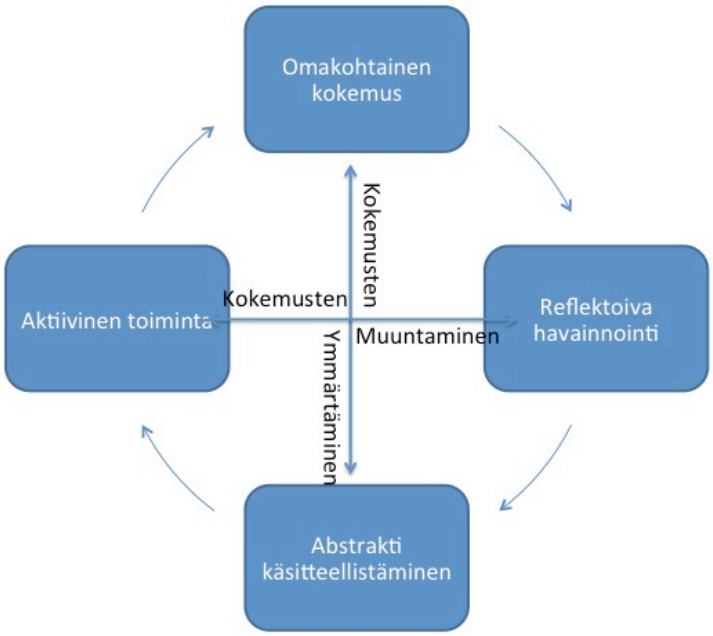
Toimintatutkimukseen perustuvassa kehittämistyössä tutkija pyrkii siis ratkaisemaan jonkin ongelman osallistumalla tutkittavan organisaation toimintaan sen muiden toimijoiden kanssa. Usein toimintatutkimukseen liittyy jokin käytännönläheinen ja kohteelle relevantti ratkaistava asia. Keskeinen ero on, että tutkija on osa tutkimuskohdetta, ei etäinen tarkkailija. ”Toiminta perustuu itsereflektioon ja itsearviointiin praktisen päättelyn perusteella” (Eskola & Suoranta 2005, 128).

Toimintatutkimuksessa pyritään siis käytännönläheiseen organisaation kehittämiseen aktiivisesti itse osallistuen. Tähän kehittämistyöhön tutkimusmenetelmäksi valittua toimintatutkimusta voidaan perustella tutkimuksen lopputuloksen tavoitteen kautta. Tavoitteena on kehittää poliisihallintoa siten, että ulkoisesti asetettu vaatimus tietoturvallisuudelle täyttyy toimien samalla yhtenä tasavertaisena organisaation jäsenenä.

4.1.1 Toimintatutkimus oppimisprojektina

Toimintatutkimuksen yksi perusperiaate on, että ihminen on aktiivinen oppija ja että hänellä on motivaatio kehittää omaa työympäristöään. Toimintatutkimuksen yksi tavoite onkin lisätä tietoisuutta ja aktivoida ihmistä muutostyöhön (Jyrkämä 1978, 64-65). Tavoitteen kannalta lähestymistapa on oivallinen, sillä tietoturva-asetuksen vaatimukset vaikuttavat laajaa joukkoa poliisin henkilöstöä ja konkretisoituvat juuri uusien toimintatapojen omaksumisena yksittäisen työntekijän tehdessä työtään. Aktiivinen kokemuksellinen oppiminen tarvitsee kuiten-

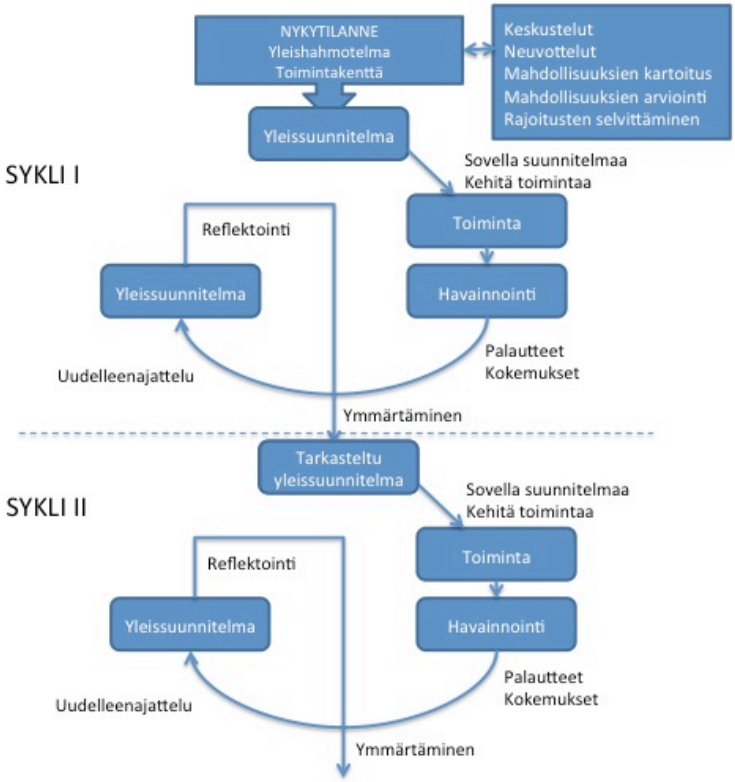
kin jatkuvaa toiminnan havainnointia ja reflektointia jolloin toimintatutkimuksen tutkija on kehittämisprosessin muutosagentti ja ylläpitäjä (kuva 4) (Kolb 1984, 42).



Kuva 4: Kokemuksellisen oppimisen malli (Tertsunen 1999)

4.1.2 Toimintatutkimuksen kehittämisprosessi

Toimintatutkimusta kuvataan usein spiraalimaisena syklinä jossa empiirinen kenttätyö ja kriittinen tutkimuksen arviointi vuorottelee. Syklit syventävät tutkimuksen tietoa tutkittavasta – ja kehitettävästä kohteesta kokemuksien karttuessa. Jokainen sykli pureutuu kerroksittain tutkittavaan asiaan syvemmälle ja luo samalla pohjaa seuraavalle syklille (kuva 5). Jotta tutkimusta voitaisiin kutsua toimintatutkimukseksi, sykleissä tulee toistua vaiheet suunnittelu, toiminta, havainnointi ja reflektointi (Katila & Meriläinen 2006, 138).



Kuva 5: Toimintatutkimuksen spiraali (Tertsunen 1999)

4.2 Kehittämisprosessi poliisihallinnon kehittämistapauksessa ja rajoitteet

Tietoturva-asetuksen kehittämisprosessin I sykli poliisihallinnossa voidaan jakaa toimintatutkimuksen malliin seuraavasti.

- **Suunnittelu**vaiheessa tunnistettiin tietoturva-asetuksen vaatimukset, arvioitiin poliisihallinnon nykytila suhteessa tietoturva-asetuksen vaikutuksiin, toteutettiin karkean tason kehittämissuunnitelma sekä valmisteltiin ohjeistus vaatimusten täyttämiseksi.
- **Toiminta**vaiheessa kehittämissuunnitelman toimenpiteitä sekä valmisteltu ohjeistus jalkautettiin ja toimintaa korjattiin vaatimusten mukaiseksi.
- **Havainnointi**vaiheessa vedettiin yhteen saatu palaute ja arvioitiin toimintavaiheen korjausten riittävyys suhteessa vaatimuksiin.
- **Reflektointi**vaiheessa kehittämissuunnitelmaa parannettiin palautteen ja arviointien perusteella.

Toimintatutkimuksen kannalta voidaan poliisihallinnon todeta olevan tarkasteluhetkellä joulukuussa 2012 toteuttanut I syklin ja parhaillaan II syklin alussa, parannellun kehittämissuunnitelman käyttöönottovaiheessa.

Ajallisena lähtökohtana tämän työn kehittämisprosessille pidetään tietoturva-asetuksen voimaantuloa ja sitä edeltävää valmisteluprosessia vuonna 2010. Kehittämistyön keskeisiä rajoitteita on asetuksen siirtymäsäännöksen aikataulut, perustaso tulee saavuttaa 30.9.2013 ja korkeammat tasot 30.9.2015. Muita rajoitteita ovat tietoturva-asetuksen asettamat vaatimukset sekä käytettävissä olevat resurssit kehittämistyöhön.

5 Vaatimusten tunnistaminen ja toimenpiteiden suunnittelu (sykli I, suunnittelu)

5.1 Tietoturva-asetuksen voimaantulo ja alustavat toimenpiteet

Tietoturva-asetusta valmisteltiin valtionhallinnossa Oikeusministeriön johdolla useita vuosia ja sen aikataulusta tavattiin useita erilaisia käsityksiä vielä alkuvuonna 2010. Asetuksen voimaantuloon ei varauduttu aktiivisesti sisäasiainhallinnon vuoden 2010 vuosisuunnittelussa sen aiempien lykkääntymiskokemusten vuoksi. Varmistettu tieto asetuksen hyväksynnästä ja pikaisesta voimaantulosta saavutti sisäasiainhallinnon keväällä 2010 jonka jälkeen asetuksen vaatimia kehittämistoimia ryhdyttiin tarkemmin suunnittelemaan.

5.2 Tietoturva-asetuksen vaatimien toimenpiteiden suunnittelu

Tietoturva-asetuksen vaatimien toimenpiteiden suunnitteluun ryhdyttiin siis arvioimalla karkealla tasolla ensin poliisihallinnon tietoturvallisuuden nykytila suhteessa vaatimuksiin. Kun tunnistettiin, että työ tulisi vaatimaan sekä tietoaineistojen luokitteluohjeistuksen uudistamisen että laajemmin toimintatapoja ja joidenkin konkreettisten tekniikkaa koskevien vaatimusten täyttämistä, oli mahdollisuus suunnitella ja aikatauluttaa toimenpiteet.

Kehittämistyö jaettiin alustavasti kahteen samanaikaisesti toteutettavaan osaan. Ensimmäinen osa käsittäisi aiemmin voimassa olleen tietoaineiston luokittelumallin ja käsittelyohjeistuksen päivittämisen sekä kouluttamisen henkilöstölle. Toinen osa vastaisi tietoturva-asetuksen tietoturvatasovaatimusten jalkauttamiseen poliisihallintoon. Kuvassa 6 on karkealla tasolla kuvattu alustava suunnitelma, miten tietoturva-asetuksen vaatimukset pyrittiin poliisihallinnossa toteuttamaan siirtymäaikojen puitteissa.

Kuva 6: Tietoturva-asetuksen käyttöönoton suunnitellut toimenpiteet karkealla tasolla

Aikataulullisesti toimintatutkimuksen I sykli suunniteltiin siis seuraavasti:

- **suunnittelu** ja ohjeistuksen valmistelu pääsääntöisesti vuoden 2010 aikana;
- **toteutus**vaihe 2011-2012;
- **havainnointi** ja palautteiden yhteenveto kevät 2012;
- **reflektointi** ja tarkennetun suunnitelman tekeminen syksy 2012.

Tavoitteeksi asetettiin, että I syklin jälkeen poliisihallinnossa täyttyisi tietoturva-asetuksen määrittämä perustaso 1.1.2013, kymmenen kuukautta ennen tietoturva-asetuksen siirtymäjakson päättymistä. Ajankohta katsottiin hyväksi pisteeksi myös todeta korjaavat toimenpiteet mikäli perustaso ei vielä kaikilta osin täyttyisi. Vuodenvaihde 2013 aloittaisi myös toimintatutkimuksen toisen syklin jossa tavoitteena olisi kehittää toimintaa edelleen korotetun tason saavuttamiseksi ja kokemusten perusteella tarkentavien tai korjaavien toimenpiteiden suorittaminen ensimmäisen vaiheen tulosten perusteella. II sykli suunniteltiin aikataulullisesti alustavasti seuraavasti:

- **suunnittelu** loppuvuosi 2012;
- **toteutus** alkuvuodesta 2013 kevääseen 2014;

- **havainnointi** ja tilanteen yhteenveto kesällä 2014;
- **reflektointi** ja tarkennetun suunnitelman tekeminen syksy 2014.

5.3 Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä

Tietoturva-asetuksen siirtymäaika alkaa kulua viranomaisen tekemästä tietoaineistojen luokittelupäätöksestä. Sisäasiainhallinnossa oli ainakin jo ennen tietoturva-asetuksen voimaantuloa vuodelta 2006 määräys asiakirjojen luokittelusta ja salassa pidettävien asiakirjojen käsittelystä (Sisäasiainministeriön määräys salassa pidettävien tietoaineistojen luokittelusta ja käsittelystä 2006.), todennäköisesti pidempäänkin. Koska tietojen luokittelupäätös sisäasiainhallinnossa oli siis tehty jo ennen asetuksen voimaantuloa, tulkittiin sisäasiainhallinnossa asetuksen siirtymäajan alkaneen asetuksen voimaan tulon yhteydessä 1.10.2010 jo ilman erityistä uutta päätöstä.

Sisäasiainministeriön määräys oli jalkautettu myös aiemman poliisin hallintorakenteen mukaisesti silloin poliisin ylijohtona toimineen Sisäasiainministeriön poliisiosaston määräyksenä poliisihallinnon tietoturvaperiaatteet osana poliisihallintoon (Poliisihallinnon tietoturvaperiaatteet 2008). Luokittelu oli turvallisuusviranomaisten yleisesti käyttämä neliportainen ns. turvallisuusluokittelumalli:

- Turvallisuusluokiteltu TLL I ERITTÄIN SALAINEN
- Turvallisuusluokiteltu TLL II SALAINEN
- Turvallisuusluokiteltu TLL III LUOTTAMUKSELLINEN
- Turvallisuusluokiteltu TLL IV VIRKAKÄYTTÖ

(Poliisihallinnon tietoturvaperiaatteet 2008).

Luokittelussa oli tunnistettu haastavaksi, että turvallisuusluokkaa IV ei laajasti tunnettu tai osattu käyttää. Luokan IV käyttö oli myös julkisuusasetuksen mukaisesti ongelmallinen, koska sitä ei tunnistettu lainsäädännössä. Lisäksi osa poliisin yksiköistä ja toiminnoista käytti salassa pidettävien asiakirjojen salaamisessa laajasti leimaa ”SALASSA PIDETTÄVÄ” jossa ei määritelty turvallisuusluokkaa lainkaan.

Uuden luokittelun työstämiseksi otettiin pohjaksi sisäasiainministeriön vanha määräys. Määräysluonnos valmisteltiin luokittelun osalta vastaamaan tietoturva-asetusta ja samalla määräyksen käsittelyvaatimukset arvioitiin uudelleen erityisesti VAHTI 2/2010 ohjeen vaatimuksia peilaten.

Määräystä valmisteltiin vuonna 2010 ensin hallinnonalan yhteisenä määräysluonnoksena sisäasiainministeriön hallinnonalan eri toimialojen yhteistyönä. Kun määräysluonnos oli saatu

pääsääntöisesti kaikkia tyydyttävälle tasolle, se siirrettiin syksyllä 2010 poliisihallinnon sisäiseen valmisteluun tavoitteena valmistella luonnoksesta poliisihallinnon määräys. Muut sisäasiainhallinnon toimialat toimivat tahoillaan samoin.

Luonnoksesta pyydettiin lausunnot poliisin yksiköiltä loka-marraskuussa 2010 ja kommenttikierroksen muutosten jälkeen se käsiteltiin poliisin yhteistoimintaryhmässä 14.12.2010. Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä (2020/2010/4030) hyväksyttiin muutosten jälkeen voimaan 1.1.2011 (liite 1).

5.4 Tietoturvallisuuden arviointi ja määräys tietoturvatasot poliisihallinnossa

Jotta tietoturva-asetuksen toinen keskeinen vaatimus, tietoturvallisuuden kypsyystasot, eli tietoturvatasojen toimenpiteet saataisiin suunniteltua ja jalkautettua poliisiin, todettiin keväällä 2010 että poliisihallinnon tietoturvallisuuden nykytaso suhteessa tietoturvatasojen vaatimuksiin tulisi arvioida. Poliisihallintoon oli Valtiokonttorin toimesta tehty vuonna 2009 tietoturvatasoarviointi perustasoa vasten, jonka mukaan poliisihallinto pääsääntöisesti täyttäisi vaatimukset. Valtiokonttorin arvioinnin tuloksia pidettiin kuitenkin hieman pintapuolisesti laadittuna jotta niihin voisi täysin luottaa.

Huhtikuussa 2010 toteutettiin Poliisihallituksessa tietoturvatasojen itsearviointi, jossa todettiin keskeiset puutteet ja jonka perusteella suunniteltiin toimenpiteet tietoturvatasotyölle. (Poliisin tietoturvatasoauditointiraportti 2010)

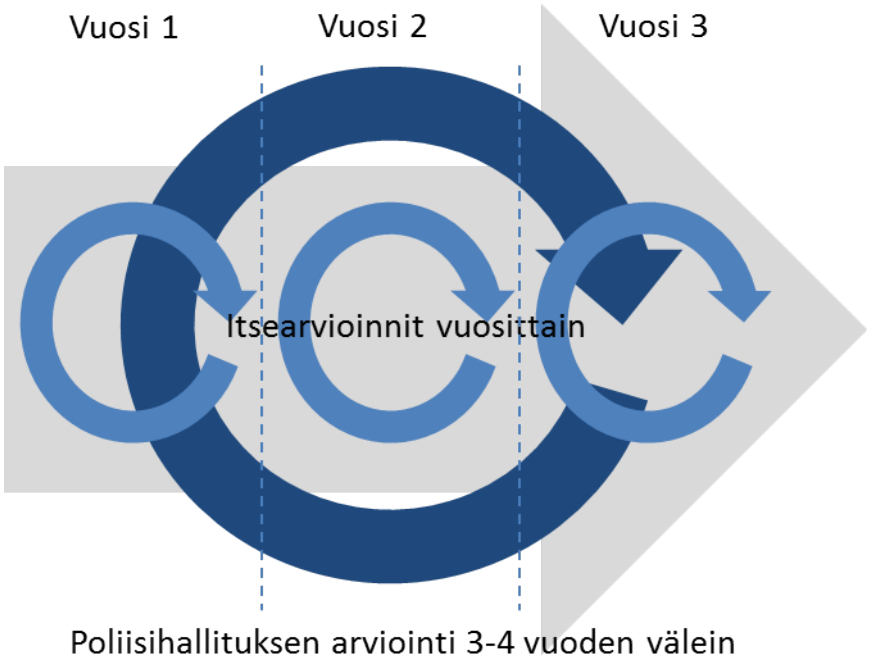
Tunnistettujen puutteiden perusteella, vuoden 2010 aikana, kahdessa poliisin yksikössä tehtiin Poliisihallituksen ohjeistamana ja Poliisihallituksen tietoturvapäällikön kanssa yhteistyössä tietoturvatasojen itsearviointi ja aloitettiin tietoturvatasojen kehittämistyö pilottimallisesti.

Kehittämistyöstä saatujen kokemusten perusteella valmisteltiin Poliisihallituksessa syksyn 2010 aikana määräys Tietoturvatasot poliisihallinnossa (2020/2011/81, liite 2) joka saatettiin voimaan tammikuussa 2011. Määräyksen tarkoituksena oli ohjeistaa ja vastuuttaa poliisin yksiköille tietoturvallisuuden arviointi- ja kehittämistehtävät tietoturva-asetuksen vaatimusten täyttämiseksi.

Lähtökohtana määräyksen ohjeistamassa tietoturvatasotyössä pidettiin yksiköissä itsenäisesti tapahtuvaa itsearviointia ja kehittämistyötä. Poliisihallituksen tietoturvaresurssien vähyyden ja poliisin yksiköiden suuren lukumäärän vuoksi ei tietoturvatasojen kehittämistyössä voitu toteuttaa täysin konsernijohtoisena. Lisäksi yksiköiden turvallisuuden hallinnan toimintatavat poikkesivat toisistaan jonkin verran, mikä olisi osaltaan tuottanut lisätyötä konsernimaisessa

painotuksessa. Koko poliisihallintoa koskevissa ja muuten yhtenevissä asioissa suunniteltiin ja ohjeistettiin Poliisihallituksen kuitenkin toteuttavan yhteisen ohjeistuksen tai muun kehittämistyön kunhan yksiköt tunnistaisivat arviointien perusteella kehittämistarpeita.

Yksiköiden vuosittain toteuttamien tietoturvallisuuden itsearviointien tukemiseksi suunniteltiin 3-4 vuoden välein tapahtuva ulkoinen, Poliisihallituksen toteuttama tarkastus (kuva 7). Ulkoinen tarkastus on myös yksi tietoturvatasojen vaatimuksista joka täytettiin näin toteuttaen.



Kuva 7: tietoturvatasojen arviointi poliisihallinnossa

Määräyksen valmistelun yhteydessä poliisin ylin johto teki linjauksen poliisihallintoon tavoiteltavasta tietoturvatasosta, poliisihallinnon tietoturvallisuuden haluttiin olevan vähintään korotetulla tasolla määräyksen siirtymäajan kuluessa. Kirjaus sisällytettiin myös tietoturvatasot poliisihallinnossa määräykseen.

Tavoite korotetusta tasosta perustui siihen, että pääosa yksiköistä käsittelee jatkuvasti suojaustason III salassa pidettävää aineistoa (esimerkiksi pääsääntöisesti esitutkinta- ja lupahallinnon työ) kun taas suojaustason II tai sitä korkeampaa tietoa käsitellään selvästi rajoitetummin. Niille poliisin yksiköille tai yksiköiden osille, jotka käsittelevät usein suojaustasojen I tai II tietoja, annettiin ohjeistus määrittää toiminta itsenäisesti korkealle tasolle.

Määräyksellä annettiin yksiköille vaatimus arvioida oma tietoturvallisuuden tasonsa suhteessa VAHTI 2/2010 ohjeen tietoturvatasovaatimuksiin ja toteuttaa tietoturvatasojen perustasojen

vaatimukset vuoden 2012 loppuun mennessä sekä korotetun tason vaatimukset vuoden 2014 loppuun mennessä. Tietoturva-asetuksen siirtymäajat ovat 1.10.2013 perustaso ja 1.10.2015 korkeammat tasot. Siirtymäajan lyhentämisellä poliisihallinnossa haluttiin varautua mahdollisiin poikkeamiin joita saatettaisiin tunnistaa arviointityön aikana ja mahdollisuuteen korjata puutteita vielä 10 kuukauden aikana ennen asetuksen määrittämän siirtymäaikojen päättymistä.

Tietoturvatasotyö rajattiin siten, että kaikki poliisin yksiköt vastuutettiin arviomaan ja toteuttamaan vähintään VAHTI 2/2010 liitteen 5 (Tietoturvatason yksityiskohtaiset vaatimukset) luvun 1 (Tietoturvallisuuden hallinnan vaatimukset). Poliisihallinnossa suuri osa tietohallinnosta on vahvasti konserniohjattua Poliisihallituksesta tai Sisäasiainministeriöstä ja tuotetaan poliisista ulkoistettuna Hallinnon tietotekniikkakeskuksen (HALTIK) toimesta. Vain rajallisella osalla yksiköistä on omia tietojärjestelmiä tai tietojärjestelmähankkeita, joten tietojärjestelmiin kohdistuvat luvun 2 (Tietojärjestelmien hallinnan vaatimukset) vaatimukset rajattiin koskemaan vain tällaisia yksiköitä. Yksiköiden tuli itsearvioinnin yhteydessä tunnistaa, onko niillä tietojärjestelmiä, joiden omistajina ne toimivat.

6 Tehdyt toimenpiteet asetuksen käyttöönotoksi (sykli I, toteutus)

6.1 Luokittelumääräyksen jalkauttaminen hallinnossa

Jotta 1.1.2011 voimaan tullut määräys poliisin salassa pidettävien tietoaineistojen käsittelystä saatiin riittävän tehokkaasti jalkautettua hallintoon, suunniteltiin siihen liittyvä koulutus pidettäväksi vuoden 2011 aikana. Koulutus koostui kolmesta keskeisestä elementistä.

- Turvallisuushenkilöstön kouluttaminen ja yksiköiden henkilöstökoulutukset
- Tietoturvallisuuden verkkokoulutus
- Muut toimenpiteet

6.1.1 Turvallisuushenkilöstön kouluttaminen ja henkilöstökoulutukset

Jokaisessa poliisin yksikössä on nimetty tietoturvapäällikkö tai -vastaava joka vastaa yksikön turvallisuuden seurannasta ja kehittämisestä mukaan lukien henkilöstön kouluttamisesta. Tälle henkilöstölle järjestetään Poliisihallituksen toimesta säännöllisesti koulutusta ajankohtaisista turvallisuuteen liittyvistä asioista.

Määräyksen henkilöstökoulutus yksiköissä suunniteltiin toteutettavaksi yksiköiden tietoturvapäälliköiden tai –vastaavien toimesta ja heille laadittiin Poliisihallituksen toimesta valmis koulutuspaketti pidettäväksi yksiköissään. 2-3. helmikuuta 2011 pidetyssä poliisin turvallisuus- ja

tietoturvaseminaarissa koulutuspaketti esiteltiin ja koulutettiin tietoturvapäälliköille ja -vastaaville. Koulutuspaketti jaettiin myös poliisin intranetjärjestelmän Seitin kautta henkilöstön tutustuttavaksi.

6.1.2 Tietoturvallisuuden verkkokoulutus

Sisäasiainministeriön hallinnonalalla on ollut vuodesta 2008 tietoturvallisuuden verkkokoulutusjärjestelmä, minkä sisältämän tietoturvaosion suorittaminen on määrätty pakolliseksi kaikille hallinnonalan palveluksessa oleville. Järjestelmään suunniteltiin myös uuden salassapitomääräyksen koulutus toteutettavaksi jatkokurssiksi (kuva 8). Peruskurssi sisältää yleistä tietoturvatietämystä, kuten apua hyvän salasanan valintaan tai tietoa miten välttää roskapostia. Verkkokoulutusjärjestelmä mahdollistaa suoritusten seurannan henkilötasolla sekä lukijan oppimisen testaamisen väli- ja lopputestin muodossa.

Kuva 8: Sisäasiainhallinnonalan tietoturvallisuuden verkkokoulutusjärjestelmän jatkokurssin aloitussivu

Sisäasiainhallinnonalan salassa pidettävien tietoaineistojen käsittely- ja luokittelumääräyksestä laadittiin verkkokoulutusmateriaali ja sen suorittaminen määrättiin Sisäministeriön kanslipäällikön allekirjoittamalla kirjeellä ja poliisihallinnossa Poliisihallituksen saatekirjeellä lisättynä pakolliseksi jokaiselle sisäasiainhallinnonalan palveluksessa olevalle.

Verkkokoulutus tuli toteuttaa vuoden 2011 aikana, 31.12.2011 mennessä ja sen jälkeen kahden kuukauden kuluessa virkasuhteen aloittamisen jälkeen. Suoritusten seuranta verkkokoulutusjärjestelmästä vastuutettiin yksiköiden tietoturvapäälliköille ja –vastaaville.

6.1.3 Muut toimenpiteet

Määräyksen jalkauttamiseksi tehtiin myös lukuisia pienempiä muita toimenpiteitä, kuten ohjeistettiin uusien salassapitoleimasimien tilaaminen ja erityisesti vanhojen kerääminen pois yksiköiden tietoturvapäälliköiden ja –vastaavien toimesta. Tällä toimenpiteellä haluttiin välttyä tilanteesta että osa yksiköiden henkilöstöstä jatkaisi vanhojen leimojen käyttöä eivätkä opettelisi lainkaan uusia leimoja.

Jalkauttamisen tueksi toteutettiin myös käyttäjän pikaopas luokitteluun, missä kuvattiin leimat ja perusteet eri suojaustasoille (liite 3). Pikaopasta jaettiin sähköisesti intranetissä ja yksiköiden tietoturvapäälliköiden ja -vastaavien kautta tulostettuna henkilöstölle.

Määräyksestä laadittiin Poliisihallituksen viestinnän toimesta vuonna 2011 myös useita tiedotteita poliisin intranetjärjestelmään Seittiin, jolla pyrittiin säännöllisesti muistuttamaan paitsi uudistuneesta luokittelusta ja siihen liittyvästä ohjeistuksesta että pakollisesta verkkokoulutuksesta.

6.2 Tietoturvatasot poliisihallinnossa määräyksen jalkauttaminen

6.2.1 Turvallisuushenkilöstön kouluttaminen

Tietoturvatasot poliisihallinnossa määräys koulutettiin poliisin turvallisuus- ja tietoturvapäälliköille helmikuussa 2011 pidetyssä poliisin turvallisuus- ja tietoturvaseminaarissa. Seminaarissa tietoturvapäälliköitä ja -vastaavia kannustettiin ryhtymään pikaisesti työhön, tutustumaan tietoturvatasovaatimuksiin ja organisoimaan tietoturvallisuuden kehittämistyön siten, että yksikössä heidän apunaan toimii jonkinlainen työryhmä tai muu orgaani jossa yksikön keskeiset toiminnot ovat edustettuna.

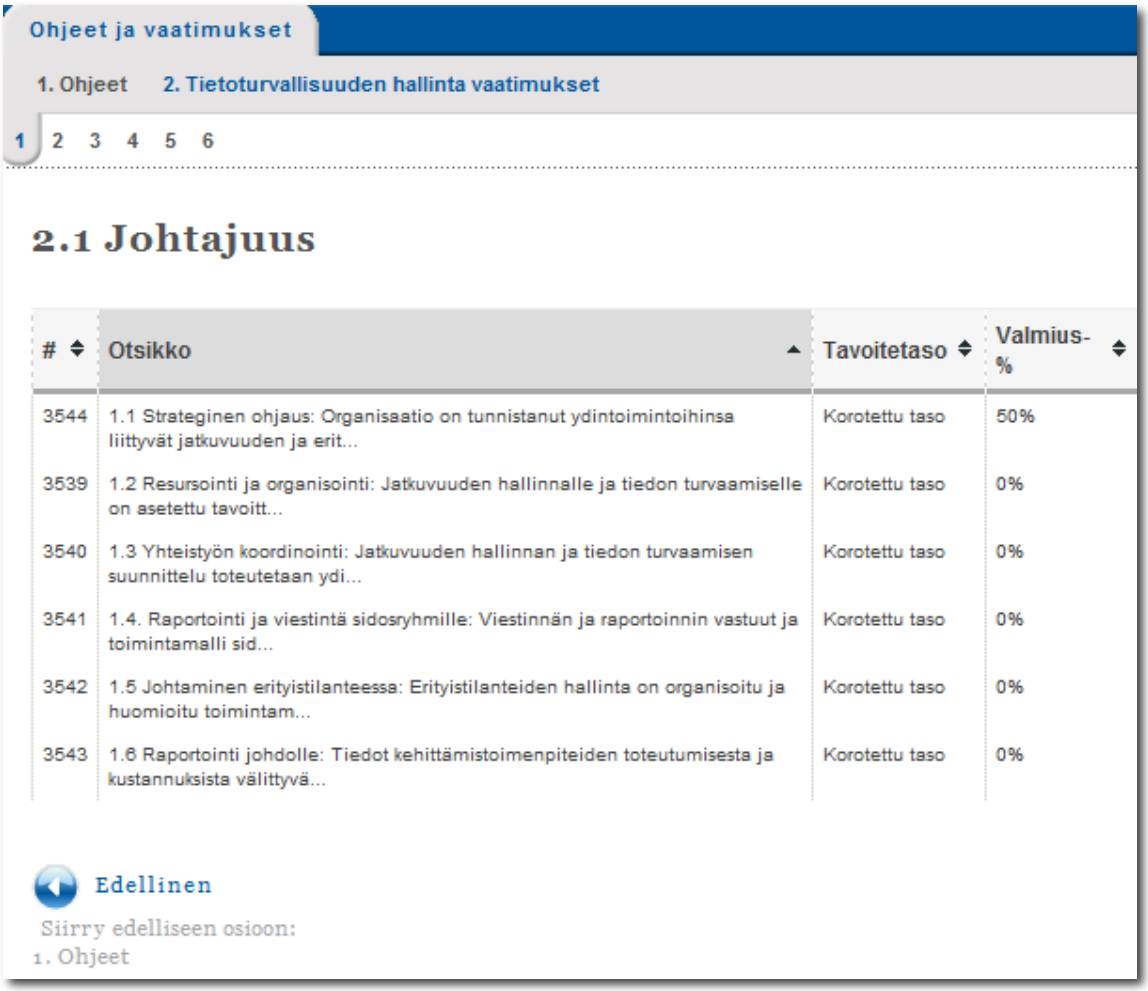
6.2.2 Tietoturvatasotyökalu

Jotta poliisin yksiköiden toteuttamat tietoturvatasojen itsearvioinnit saatiin helposti yksiköissä ja Poliisihallituksessa seurattavaan muotoon ja vertailukelpoiseksi keskenään, Poliisihallituksen toimesta hankittiin kehittämistyöhön myös yhteinen tietojärjestelmä (kuva 9). Tietojärjestelmä otettiin käyttöön ja koulutettiin helmikuun 2011 turvallisuus- ja tietoturvaseminaarin yhteydessä.

Kuva 9: Näkymä tietoturvatasotyökalun aloitussivulta

Tietojärjestelmän idea oli, että yksiköiden tietoturvapäälliköt ja -vastaavat saavat tietoturvatasojen hallinnolliset sekä tietojärjestelmien vaatimukset käsiteltäväkseen. Halutessaan yksiköillä oli mahdollisuus pyytää muillekin tietoturvatasoja kehittäville tahoille oikeuksia järjestelmään, jotta arviointi- ja dokumentointityötä saatiin tehtyä laajemmin kuin yhden vastuuhenkilön toimesta. Näin toimittiinkin useimmissa yksiköissä.

Tietoturvatasotyökalu suunniteltiin seuraavasti; Kuhunkin vaatimukseen tuli määrittää toteutuuko vaatimus vai ei, vai onko joku syy miksi vaatimus ei koske kyseistä yksikköä. Lisäksi vaatimukseen tuli asettaa vastuuhenkilö ja aikataulu, mikäli vaatimus ei täyttynyt. Tämän lisäksi jokaisella vaatimuksella oli kommenttikenttä johon määritettiin perusteet miksi vaatimus täyttyi tai ei sekä suunnitellut toimenpiteet. Järjestelmä laski automaattisesti kunkin tietoturvatasojen päävaatimuksen valmiusasteen prosenteissa (kuva 10). Yksikkö pystyi näkemään myös kokonaisprosentin kaikkien vaatimusten toteutumisesta. Poliisihallitus näki omasta näkymästään kaikkien yksiköiden valmiusasteen ja pystyi halutessaan pureutumaan tarkemmin yksittäisen yksikön vastauksiin.



Kuva 10: Tietoturvatasotyökalun vaatimusten yleisnäkymä (valmiusasteet esimerkkejä)

7 Tietoturva-asetuksen kokemuksia ja korjaavia toimenpiteitä (sykli I, havainnointi)

Toimintatutkimuksen menetelmin tehtävässä kehittämistyössä jatkuva arviointi ja toiminnan kehittäminen kokemusten ja saadun palautteen perusteella kuuluu osaksi prosessia. Kuten aktiivisessa ja ohjeistusta toimintaansa soveltavassa organisaatiossa voidaan olettaa, palautetta suunnitelluista ja tehdyistä toimenpiteistä on saatu heti jo ennen tutkimuksen havainnointivaihetta, suoraan mahdollisten ongelmien esiintyessä. Merkittävä osa konkreettisista palautteista on korjattu tai alettu korjaamaan jo heti palautteen saamisen jälkeen. Keväällä 2012 tehtiin kuitenkin yhteenveto saadusta palautteesta ja ongelmista. Näistä keskeiset on kuvattu alla asiaa konkretisoivin esimerkkitapauksien avulla.

7.1 Palaute poliisin salassa pidettävien tietoaineistojen käsittelymääräyksestä

Määräyksen valmistelun yhteydessä määräysluonnoksesta pyydettiin lausunnot Sisäasiainministeriön poliisiosastolta, Hallinnon tietotekniikkakeskus HALTIKista sekä poliisin yksiköiltä. Lau-

sunnoissa yhtenevää oli, että pelättiin yksityiskohtaisten käsittelyvaatimusten hankaloittavan päivittäisen poliisityön tekemistä ja tuovan kustannuksia kun erilaisia kehittämistoimenpiteitä joudutaan tekemään.

Määräysluonnokseen tehtiin lausuntojen perusteella joitakin kevennyksiä suhteessa VAHTI 2/2010 ohjeen vaatimuksiin riskianalyysiin perustuen salassa pidettävän aineiston laajan käsittelyn vuoksi. Esimerkiksi VAHTI 2/2010 ohjeessa vaaditaan ”Luokitellut (suojaustasot I – III) paperimuotoiset asiakirjat on säilytettävä vähintään Euro II -normin mukaisessa data- tai kassakaapissa sen mukaan, mikä asiakirjan suojaustaso on.” (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 71.)

Mm. Edellä mainitun vaatimuksen kirjaimellinen täyttäminen olisi käytännössä vaatinut usean tuhannen euron kassakaapin hankintaa pääosaan poliisihallinnon huoneista sekä lukuisten poliisitalojen rakenteiden vahvistamista kassakaappien aiheuttaman painon vuoksi. Poliisihallinnossa määriteltiin että suojaustason III aineistoja voidaan säilyttää lukitussa kaapissa poliisitalon muun rakenteellisen suojauksen vuoksi ja lujempia ratkaisuja vaadittaisiin vasta suojaustasolta II. Vastaavanlaisia muutoksia vaatimuksiin toteutettiin muutamia.

Erityinen havainto lausuntokierrokselta oli, että useissa kommenteissa suhtauduttiin kriittisesti myös käsittelyvaatimuksiin jotka olivat olleet voimassa jo vuosia aiemmissa määräyksissä asetettuna. Voitaneenkin päätellä, että aiempien määräysten jalkauttaminen poliisihallinnossa ei ole ollut täysin kunnossa koska lausuntoja antaneet virkamiehet eivät tienneet kaikista jo voimassa olevista vaatimuksista. Tällainen usein toistuva kriittinen kommentti koski mm. vaatimusta suojaustason III salassa pidettävän tietoaineiston sähköpostiviestin salaamista sisäverkossa.

Muita keskeisiä kritiikin kohteena olevia asioita olivat tietoturva-asetuksen määrittämä luokittelumalli ja siihen liittyvät vaatimukset. Neljäportainen ja kahdeksanleimainen luokittelumalli koettiin lausunnoissa erittäin sekavaksi ja vaikeaksi omaksua. Koska luokittelumalli tuli tietoturva-asetuksen osana, ei Poliisihallituksella ollut mahdollisuutta vaikuttaa asiaan muutoin kuin lisäkoulutuksen ja ohjeistuksen avulla. Poliisihallituksessa suunniteltiinkin käyttäjän huoneentaulu luokittelun tekemiseksi ja käsittelyvaatimusten muistin virkistämiseksi (liite 3).

7.1.1 Kokemukset salassapitomääräyksen koulutuksista

Tammikuussa 2011 salassapitomääräyksen voimaantulon jälkeen määräyksen kouluttamisesta alkoi saapua koulutuspyyntöjä Poliisihallitukseen. Koulutuspyyntöjä osattiin jonkin verran odottaa ja koulutuksia ehdotettiinkin yksiköihin mutta pyyntöjen suuri lukumäärä yllätti. Lukuisten poliisin yksiköiden tekemien pyyntöjen lisäksi tarve koulutuksille ilmeni erityisiltä

ammattiryhmiltä kuten esimerkiksi tutkinnanjohtajilta, tutkintasihteereiltä ja tietojärjestelmähankehenkilöstöltä.

Koulutuksia pidettäessä ilmeni, että koska määräys oli luonnosteltu yleiseksi, koko sisäasianhallinnon toimialat kattavaksi, sen konkreettisuudessa oli jouduttu mahdollisesti liikaa karsimaan. Palautetta ja kritiikkiä ilmaantui erityisesti rikostutkinnan tietojen luokittelusta ja käsittelyvaatimuksista, joka olikin määräyksessä kevyemmin ohjeistettu. Toki asiaa on tarkennettu poliisin toiminnallisissa ja muissa ohjeissa.

Selkeä viesti oli, että poliisihallinnossa henkilöstö on tottunut selkeään ja konkreettiseen ohjeistukseen, missä virkamiehen omalle tulkinnalle ei jätetä tarpeettoman laajasti mahdollisuutta. Toisaalta poliisihallinnon henkilöstö on tottunut arvioimaan ja ohjaamaan toimintaansa myös suoraan lainsäädännön kautta mikä jättää tulkinnan varaa toiminnalle vielä enemmän.

Keväällä 2011 Poliisihallituksessa tunnistettiin myös, että vaikka yksiköiden tietoturvapäälliköille ja –vastaaville oli helmikuussa järjestetty oma koulutustilaisuus (turvallisuus- ja tietoturvaseminaari), ei osaaminen kaikkien vastuutahojen osalta ollut vielä riittävää jotta jokaisen yksikön vastuuhenkilöt olisivat pystyneet kouluttamaan henkilöstönsä. Alkukesästä 2011 tehtiin Poliisihallituksessa päätös, että Poliisihallituksen tietoturvapäällikkö tekee loppuvuoden 2011 aikana vierailun kaikkiin poliisin yksiköihin ja kouluttaa uuden määräyksen yksikön tilaisuuksiin kutsumalle henkilöstölle. Lopulta vuoden 2011 aikana Poliisihallituksen tietoturvapäällikkö vieraili yhtä lukuun ottamatta kaikissa poliisin yksiköissä pitämässä salassapitomääräykseen liittyvän henkilöstökoulutuksen. Yhteensä Poliisihallituksen tietoturvapäällikkö piti vuoden 2011 aikana yli 40 koulutustilaisuutta salassapitomääräyksestä ja tilaisuuksien henkilöstömäärät vaihtelivat vajaasta 20:sta yli 200 hengen auditorioiluentoihin.

7.1.2 Tietoturvallisuuden verkkokoulutukseen liittyvät havainnot

Vuonna 2010 tietoturvallisuuden verkkokoulutuksen seuranta yksikkö- ja yksilötasolla oli mahdollista, mutta vaati yksiköiden tietoturvapäälliköiltä ja –vastaavilta aktiivisia, työläitä toimenpiteitä. Uusi henkilöstö tuli lisätä järjestelmään manuaalisesti ja henkilöstöstä pystyi hakemaan suorituksia vasta kun anonymisoidut käyttäjätiedot oli muunnettu manuaalisesti todellisiksi käyttäjiksi. Tämä aiheutti tilanteen, jossa yhteenvetojen perusteella osa yksiköistä laiminlöi verkkokoulutuksen toteuttamista ja seurantaa.

Ennen salassapitomääräyksen koulutusmoduulin julkistamista, vuoden vaihteessa 2010–2011 järjestelmää muutettiin siten, että käyttäjätiedot haettiin automaattisesti sisäasiainhallinnon

rekistereistä ja suoritustiedot säilytettiin järjestelmässä ilman anonymisointia tulosten seurannan helpottamiseksi. Järjestelmään tehtiin myös eräitä muita kehittämistoimenpiteitä.

Palaute verkkokoulutusjärjestelmän toteutuksesta oli pääsääntöisesti erittäin positiivista ja määräajassa vuoden 2011 aikana koulutuksen toteutti lähes 100 % poliisihallinnon työssä olevasta henkilöstöstä. Poikkeuksia aiheuttivat lähinnä komennuksilla tai virkavapailla olevat henkilöt. Loppuvuonna 2011 järjestelmää kehitettiin vielä siten, että siihen lisättiin automaattinen sähköpostiheräte, mikäli henkilö ei ole suorittanut käskettyjä koulutuksia annetussa määräajassa.

7.1.3 Kokemuksia salassapitoleimasinten uusimisesta

Jotta vältyttäisiin vanhojen leimasinten käytön jatkumiselta uuden määräyksen voimaan tulon jälkeen, Poliisihallitus lähetti 20.1.2011 poliisin yksiköille kirjeen, jossa ohjeistettiin poliisin yksiköitä tilaamaan uudet leimasimet ja hävittämään vanhat yksiköiden tietoturvapäälliköiden ja -vastaavien toimesta.

Kirjeen perusteella hallinnosta kerättiin huomattava määrä vanhoja salassapidon merkintään tarkoitettuja leimasimia, joista vanhimmat edelleen käytössä olleet tunnistettiin perimätiedon mukaan olevan jopa 1930–40-luvuilta sota-ajoilta (kuva 11). Toki pääosa oli asianmukaisia aiemman normiston mukaisia leimasimia.

Kuva 11: Esimerkkejä pois kerätyistä leimasimista tai tunnistetuista merkintätavoista

Leimasinten keräyksen yhteydessä havaittiin myös, että poliisin yksiköillä oli yllättävän erilaisia tapoja leimata asiakirjoa vaikka merkintäohjeistus oli ollut pääosin samanlaisena sisäasiainhallinnon määräyksissä jo aiemmin. Ei sallittujen leimasinten pois keräämisellä saatiin todennäköisesti huomattavasti yhtenäistettyä leimausmerkintöjen tekemistapaa.

Leimasinten kerääminen aiheutti laajasti myös kyselyjä poliisin lomakkeiden ja tietojärjestelmien kehittämisestä siten, että ne tukisivat suoraan uusia leimoja tulostettaessa asiakirjoja. Palautteesta tunnistettiin että poliisin nykyiset tietojärjestelmät eivät erityisen hyvin tukeneet salassapidon merkitsemistä tulostettaviin asiakirjoihin vaan merkintä vaati useimmiten henkilöstöltä manuaalisia toimia tulostamisen jälkeen. Nämä pyynnöt toteutettiin mahdollisuuksien mukaan olemassa oleviin lomakepohjiin tai vastuutettiin kehitteillä oleviin tietojärjestelmähankkeisiin kehitettäviksi asioiksi.

7.1.4 Salatun sähköpostin lähettämiseen liittyvä palaute

Uuden salassapitomääräyksen tullessa voimaan, saapuneissa kyselyissä ja koulutustilaisuuksien yhteydessä tunnistettiin yleiseksi ongelmaksi että vaikka poliisihallinnossa oli jo useita vuosia

ollut olemassa Väestörekisterikeskuksen myöntämään virkakorttiin kytketty sähköpostin sähköinen allekirjoitus- ja salausmahdollisuus, yllättävän harvat todellisuudessa olivat lähettäneet salattuja sähköpostiviestejä tai ylipäätään osasivat käyttää salausominaisuutta. Järjestelmässä oli myös teknisiä rajoitteita mitkä aiheuttivat salatun viestin lähettämisen olevan käytännössä käyttäjän kannalta hankalaa.

Palautteen perusteella, maaliskuussa 2011 Poliisihallitus antoi Hallinnon tietotekniikkakeskukselle toimeksiannon kehittää sähköpostisalauksen ominaisuuksia siten, että lähettämiseen liittyvät hankaluudet saataisiin korjattua. Osa toimeksiannon tehtävistä saatiin valmiiksi syksyyn 2011 mennessä, osa työstettiin valmiiksi 2012 kevään aikana. Samassa yhteydessä Poliisihallitus laati puuttuneen käyttäjän ohjeen salattujen viestien lähettämisestä.

Yksi keskeinen kriittinen palaute koski myös sähköpostilla viestintää hallinnon ulkopuolelle sellaisille tahoille joilla ei Väestörekisterikeskuksen virkavarmennetta ollut saatavilla. Yllättäväksi puutteeksi havaittiin että vaikka hallinnonalalle oltiin hankittu keskitetty tietojärjestelmä ulkopuolisten käyttäjien kanssa tehtävään salattuun viestintään, ei järjestelmän käyttöönottoa oltu todellisuudessa toteutettu teknisesti siten että järjestelmän vaivaton laaja käyttö olisi ollut mahdollista. Lisäksi osa poliisin yksiköistä oli hankkinut ja ohjeistanut yksittäisiä sovelluksia paikkaamaan keskitetyn järjestelmän puutteita. Ratkaisuksi Poliisihallitus kehitti vuoden 2011 aikana olemassa olevaa keskitettyä ratkaisua ja sen käyttäjän ohjeistusta sekä hankki toisen järjestelmän erilaista käyttötarvetta varten.

7.1.5 Havaitut ulkoisten medioiden salausongelmat

Salassapitomääräyksessä ohjeistettiin myös ulkoisten massamuistien, kuten usb-muistien ja cd-levyjen salaaminen kun ne sisältävät salassa pidettäviä tietoaineistoja. Poliisihallinnon työasemilla on käytössä useampia tiedostosalainohjelmistoja, joita oletettiin henkilöstön käyttävän työssään. Kuitenkaan keskitettyä ratkaisua ei määräyksen voimaan tulon yhteydessä oltu ohjeistettu.

Määräyksen voimaan tullessa Poliisihallitukseen tuli jonkin verran kyselyitä koskien muistivälineiden salaamista ja raportoitiin sen ongelmia tai puutteita mistä voitiin päätellä että todellisuudessa kunnollisia työkaluja ulkoisten muistien salaamiseen ei ollut käytössä. Palautteen perusteella Sisäasiainministeriö antoi Sisäasiainministeriön tietoturvallisuuden ohjausryhmän pyynnöstä Hallinnon tietotekniikkakeskukselle toimeksiannon suunnitella ja hankkia ulkoisten medioiden salaamiseen soveltuvan ohjelmiston. Ohjelmistoa testattiin poliisihallinnossa Poliisihallituksessa ja Itä-Uudenmaan poliisilaitoksessa ja lopulta se hyväksyttiin tuotantokäyttöön alkuvuonna 2012.

7.2 Tietoturvatasot poliisihallinnossa määräykseen liittyvät kokemukset

Tietoturvatasojen käyttöönotto ja siihen liittyvä määräys poliisihallinnossa suunniteltiin kahdessa poliisin yksikössä saatujen kokemusten pohjalta. Yleisenä kokemuksena alkuvuoden 2011 aikana todettiin, että poliisin yksiköiden tietoturvallisuuteen käytettävät resurssit ja osaaminen vaihtelee yksiköittäin huomattavasti. Asia mikä jossakin yksikössä voidaan työstää varsin itsenäisesti, ei välttämättä onnistu toisessa yksikössä edes tuetusti. Haaste eri yksiköiden eri tasoisista valmiuksista kehittää tietoturvallisuuttansa kävi ilmi nopeasti määräyksen voimaan tulon jälkeen.

Tietoturvatasojen vaatimukset tunnistettiin myös kohtalaisen abstrakteiksi ja Poliisihallitukseen tulleiden kyselyiden perusteella paikoitellen hankalaa tietoturvan ammattitermistöä sisältäväksi, mikä osa-aikaisille tietoturvapäälliköille ja –vastaaville saattoi olla jossain määrin vierasta. Poliisihallitus tuotti kesällä 2011 ohjeen jossa avattiin tietoturvatasojen hallinnolliset vaatimukset ja suositukset kehittämistoimenpiteiksi poliisihallinnossa tutummille termeille. Ohje otettiin hallinnossa positiivisesti vastaan.

Kesällä 2011 tietoturvatasotyökalun seurantaominaisuuksien ansiosta kävi myös ilmi, että merkittävä osa poliisin yksiköistä ei ollut aloittanut tai aikatauluttanut tietoturvatasojen itsearviointia vielä lainkaan. Aikataulun kireyden (perustaso tuli saavuttaa 2012 loppuun mennessä) tunnistaen, Poliisihallituksen tietoturvapäällikkö toteutti vierailun jokaiseen poliisin yksikköön vuoden 2011 aikana jonka yhteydessä yksikön ensimmäinen itsearviointi suoritettiin ohjatusti. Vierailut tehtiin samalla kertaa salassapitomääräyksen henkilöstökoulutuksen kanssa. Vierailuissa havaittiin että osa poliisin yksiköistä oli organisoinut tietoturvatasotyön pyydetysti ja toteuttanut itsearvioinnit ammattimaisesti, osassa työ oli vielä alkuvaiheessa.

7.2.1 Kokemuksia tietoturvatasovaatimusten toteuttamisesta

Tietoturvatason kehittämistyötä koskevien palautteiden ja kyselyiden eräs keskeinen sisältö on koskenut riittävää dokumentointia ja dokumentointimuotoa. Yksiköillä ei ole ollut täyttä varmuutta mitä asioita tietoturvatasojen täyttämiseksi tulisi yksikön sisäisesti dokumentoida ja mikä dokumentoitaisiin Poliisihallituksen toimesta keskitetysti.

Palautteiden perusteella Poliisihallitus valmisteli syksyllä 2012 yksikön tietoturvamääräyspohjan, jonka yksiköt voivat ottaa käyttöön määrittäen asiakirjaan ainoastaan yksikössään muista poikkeavat asiat kuten esimerkiksi sisäisen turvallisuusorganisaation ja jo olemassa olevat ohjeet. Tuon asiakirjan ottaessaan käyttöön, yksikkö voisi dokumentoinnin osalta olettaa olevansa vähintään tietoturvatasojen hallinnollisten vaatimusten osalta korotetulla tasolla. Määräyspohja toimitettiin poliisin yksiköiden käyttöön joulukuussa 2012.

Poliisihallitus aloitti palautteen perusteella vuonna 2012 myös yleisen poliisin henkilöstön tietoturvaohjeen laatimisen, minkä tarkoituksena on tuottaa poliisihallintoon yhtenäinen henkilöstön tietoturvaohjeisto. Yksiköissä tehtyjen itsearviointien perusteella tilanne on varsin kirjava, osassa poliisin yksiköissä on hyvin kattava tietoturvaohjeisto, osassa ohjeita ei käytännössä ole riittävällä tasolla laadittu.

7.2.2 Kokemuksia tietoturvatasotyökalusta

Tietoturvatasot poliisihallinnossa määräyksen yhteydessä otettiin poliisissa käyttöön myös tietoturvatasojen dokumentointiin ja seurantaan tarkoitettu tietojärjestelmä. Järjestelmästä saatu palaute on ollut pääsääntöisesti positiivista, tosin muutamia keskeisiä puutteita siitä tunnistettiin.

Heti käyttöönoton jälkeen järjestelmästä ei saatu riittäviä raportteja ulos jotta mm. johdon raportointi olisi voitu suorittaa yksiköissä. Vika korjattiin Poliisihallituksen toimeksiannosta alkuvuonna 2011. Ongelmia tunnistettiin myös tietyissä järjestelmän epäloogisuuksissa, mikä aiheutti että harvakseltaan järjestelmää käyttävät yksiköiden tietoturvapäälliköt ja –vastaavat eivät osanneet käyttää järjestelmää oikein. Järjestelmän sovellustoimittaja toteutti käyttöohjeen järjestelmään keväällä 2011.

Osassa yksiköistä järjestelmän tietoturvataso koettiin myös liian alhaiseksi syötettävään tietoon nähden. Tällaisissa tilanteissa Poliisihallitus antoi luvan tehdä tietoturvatasoarvioinnin ja -suunnittelun Excel lomakkeille.

7.2.3 Tietojärjestelmien hallinnan kehittäminen

Koska poliisin tietojärjestelmien hallinta ja omistajuus on varsin keskitetty Poliisihallitukseen ja Sisäasiainministeriöön, myös pääosa tietoteknisistä kehittämistoimenpiteistä todettiin tehtäväksi parhaiten konsernitasolla. Pääosa poliisin yksiköistä on tunnistanut ja todennut ettei omista yhtään tietojärjestelmää, jolloin tietoturvatasot poliisihallinnossa määräyksen mukaan tietoturvatasojen tietojärjestelmien hallinnan vaatimukset eivät koskettaneet heitä.

Poliisihallituksessa tunnistettiin konsernitasolla ongelmaksi, että vaikka omistajuus ja tietojärjestelmät onkin periaatteessa tunnistettu ja määritetty, todellisuudessa tietojärjestelmien inventointi ei ollut täysin ajantasainen ja järjestelmien luokittelu oli puutteellista. Myös yksittäisiä tietojärjestelmiä tunnistettiin joille oli vaikea määrittää omistajaa. Poliisihallituksessa toteutettiin vuonna 2011–2012 laaja poliisin tietojärjestelmien inventointi- ja luokitteluhanke jossa kaikille poliisin tietojärjestelmille määritettiin tietoturva- ja kriittisyystaso sekä

yksikäsitteinen omistaja. Tietojärjestelmät dokumentoitiin yhteiseen rekisteriin, jonka ylläpidosta ja ajantasaisuuden valvonnasta jatkossa asetettiin määräys (Poliisin tietojärjestelmien käyttöönottopäätös ja järjestelmätietojen hallinta. 2012.)

Tietojärjestelmien luokitteluhankkeen yhteydessä valmisteltiin ja otettiin käyttöön poliisin tietojärjestelmäohjeistus, missä kuvattiin järjestelmien tekniset tietoturvavaatimukset eri suojaustasoille sekä tietojärjestelmien tarkastus- ja dokumentointivaatimukset. (Poliisin tietojärjestelmien tietoturvavaatimukset. 2011).

Poliisin tietojärjestelmäkokonaisuus on parhaillaan uudistumassa merkittävästi, jolloin poliisihallinnossa on voitu linjata, että uudistuvat tietojärjestelmät tulevat tietoturva-asetuksen siirtymäaikojen puitteissa täyttämään tietoturva-asetuksen vaatimukset ja vanhat järjestelmät poistuvat pääsääntöisesti käytöstä.

8 Kokemuksista oppiminen ja kehittämissuunnitelman päivittäminen (sykli I, reflektio)

Loppuvuonna 2012 tietoturva-asetuksen käyttöönoton palautteista yhteenvedon tehneenä ja kokemuksista oppineena, Poliisihallitus tarkensi tietoturvallisuuden kehittämissuunnitelmaa vuosille 2013-2015. Kehittämissuunnitelman kolme keskeisintä tarkasteltua painopistettä on kuvattu alla.

8.1 Henkilöstön ohjeistuksen kehittäminen ja hankkeiden turvallisuuskoulus

Poliisihallinnon henkilöstön todettiin palautteen ja kokemusten perusteella panostuksiin ja kuluneeseen aikaan nähden kohtalaisen hyvin sisäistäneen 1.1.2011 voimaan tulleen määräyksen poliisin salassa pidettävien tietoaineistojen käsittelystä. Mm. tämän tuloksen perusteella tietoturvaohjeistusta päätettiin syventää tuottamalla lisäohjeistusta erityisesti loppukäyttäjän tarpeiden kannalta.

Vuoden 2012 aikana Poliisihallituksessa valmisteltiin aiempia toimintakäytäntöjä dokumentoivat ja tarkentavat määräykset poliisin tietojärjestelmien käyttö ja ylläpito sekä poliisin tietoturvahäiriöiden hallinta. Nämä määräykset on tarkoitus saattaa voimaan alkuvuodesta 2013 ja kouluttaa henkilöstölle vastaavalla menettelyllä kuin poliisin salassa pidettävien tietoaineistojen käsittelymääräys aiemmin. Vuonna 2013 on tarkoitus valmistella loppuun ja saada voimaan myös poliisin henkilöstön yleinen tietoturvaohje.

Oman henkilöstön lisäksi poliisin salassa pidettäviä tietoaineistoja käsittelee myös hallinnon ulkopuolisia henkilöitä erilaisissa hankkeissa tai ulkoistettujen palveluiden tuottamisen kautta. Aiemmin poliisihallinnossa turvallisuuskoulutus on kriittisimpiä kumppaneita lukuun otta-

matta pääsääntöisesti vastuutettu palvelua tuottavalle taholle turvallisuussopimuksissa, mutta tarkastushavaintojen ja muiden kokemusten perusteella koulutusvaatimus on toteutunut vaihtelevasti. Kehittämissuunnitelmaan todettiinkin yhdeksi painopisteeksi vuodelle 2013 otettavaksi hankehenkilöstön ja ulkopuolisten palveluntarjoajien turvallisuuskoulutuksen kehittäminen.

8.2 Tietoturvatasovaatimusten konkretisoiminen

Jo toteuttamisvaiheen aikana tietoturvatasojen termistö tunnistettiin haastavaksi tulkita. Poliisin yksiköissä tietoturvallisuuden itsearviointia tekevillä oli vaikeuksia ymmärtää mitä vaatimuksissa todellisuudessa edellytettiin. Poliisihallitus toteutti kesällä 2011 poliisihallinnon sisäisen ohjeistuksen vaatimusten tulkitsemiseksi mikä otettiin positiivisesti vastaan.

Osa tietoturvatasojen vaatimuksista on kuitenkin ohjeistuksen jälkeenkin niin abstrakteja, ettei niihin voi antaa yksiselitteistä tulkintaa. Tulkintaerot ja vaikeaselkoisuus ovat saadun palautteen ja kokemusten mukaan paikoin syöneet motivaatiota tehdä tietoturvatasojen kehittämistyötä ja ovat pahimmillaan aiheuttaneet turvallisuushenkilöstön rajallisten resurssien käyttämistä turhaan työhön.

Yhdeksi tietoturvallisuuden kehittämissuunnitelman painopisteeksi otettiin vuosille 2013-2014 tietoturvatasovaatimusten edelleen konkretisointi ja niiden työstäminen selkeiksi poliisin yksikköä koskeviksi vaatimuksiksi joihin kuhunkin pyritään ohjeistamaan yhdenmukaiset toimintatavat. Sellaiset asiakohdat jotka eivät kosketa poliisin yksikköä tai tehdään keskitetysti Poliisihallituksesta, jätetään selkeyden vuoksi työstettävistä vaatimuksista kokonaan pois.

8.3 Tietojärjestelmien tarkastus- ja hyväksyntäprosessin jalkauttaminen

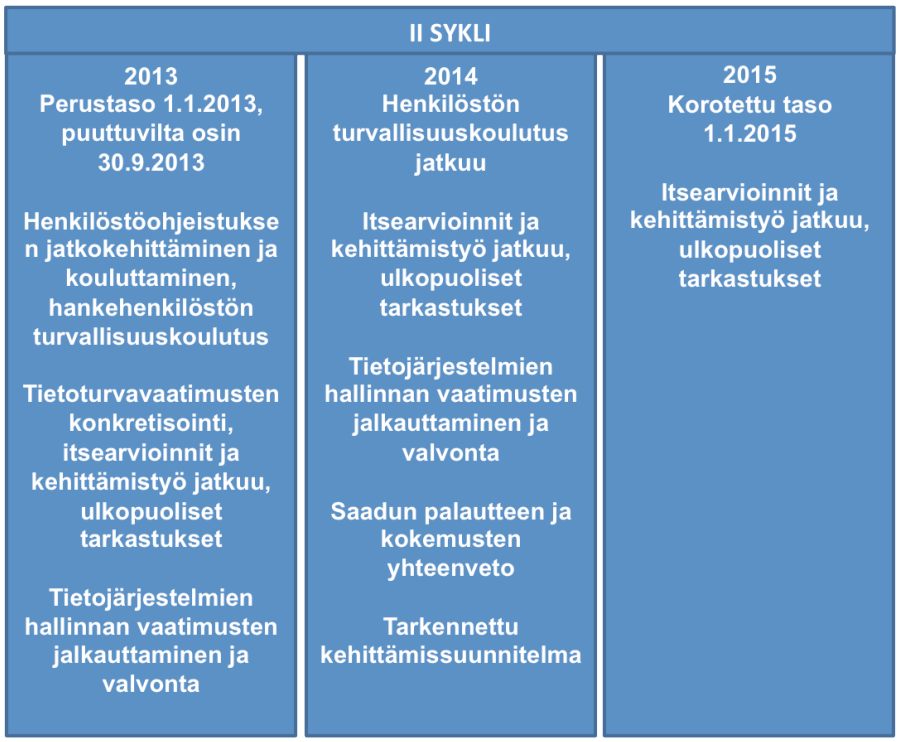
Osana tietoturvatasojen tietojärjestelmien hallinnan vaatimuksia vuosina 2011-2012 toteutettiin koko poliisihallinnon laajuinen tietojärjestelmien luokittelu- ja inventointihanke. Hankkeen tuloksina saatiin ylläpidettävä rekisteri poliisin järjestelmille ja tarkennettiin hallinnollista prosessia järjestelmien tarkastamisesta, hyväksynnästä ja dokumentoinnista. Lisäksi tuloksina saatiin yhtenäiset ja ajantasaiset mm. tietoturvatasojen kriteerit täyttävät tekniset tietoturvavaatimukset poliisin tietojärjestelmille.

Kokonaisuutena tietojärjestelmien hallinnan kehittäminen tietoturvatasojen vaatimusten mukaiseksi on edennyt aikataulussa. Koska edellä mainitut toimenpiteet muuttavat toimintatapoja ja vaatimuksia aiemmista, on niiden kouluttaminen ja valvonta vuosina 2013-2015 suunniteltu yhdeksi painopisteeksi. Vuodelle 2013 on kehittämissuunnitelmassa suunniteltu tietojärjestelmähankehenkilöstön ja palveluntarjoajien koulutustilaisuuksia. Lisäksi tietojärjes-

telmien hyväksyntäprosessia koulutetaan tietojärjestelmien omistajille. Edelleen tehtävissä tietojärjestelmätarkastuksissa huomioidaan muuttuneet kriteerit.

9 Toimenpiteiden tarkastelu vuosille 2013-2015 (sykli II)

Korjatun tietoturvallisuuden kehittämissuunnitelman mukaisesti painopisteinä vuodelle 2013 tulevat olemaan henkilöstöohjeistuksen edelleen kehittäminen ja kouluttaminen, tietoturvatasovaatimusten konkretisointityö sekä tietojärjestelmien hallinnan ohjeistuksen jalkauttaminen. Kuvassa 12 on osoitettu kuinka toimenpiteet on suunniteltu asettuvan eri vuosille.



Kuva 12: Korjattu karkean tason painotetut kehittämistoimenpiteet vuosille 2013-2015

Suunnitelma toteuttaa toimintatutkimuksen periaatteet aikataulullisesti seuraavasti:

- **suunnittelu** ja ohjeistuksen valmistelu loppuvuosi 2012- alkuvuosi 2013;
- koulutusten ja kehittämistoimien **toteutus** alkuvuosi 2013 - kesä 2014;
- **havainnointi** ja palautteiden yhteenveto kesä 2014;
- **reflektointi** ja tarkennetun suunnitelman tekeminen loppuvuosi 2014.

Keskeisiä kehittämistä ohjaavia päivämääriä syklissä II ovat tietoturva-asetuksen siirtymäajat. Perustason on täytyttävä viimeistään 30.9.2013 ja korotetun tason 30.9.2015 (poliisihallinnon sisäinen vaatimus 1.1.2015). Loppuvuonna 2014 tarkennetaan suunnitelmaa puutteiden osalta

ja tarvittavat kehittämistoimenpiteet toteutetaan vuonna 2015 alkavassa syklissä III, mikäli havaitaan ettei korotettu taso kaikilta osin täyty.

10 Johtopäätökset

Tietoturva-asetuksen täytäntöönpano poliisihallituksessa on alkuperäisen aikataulun ja siirtymäaikojen puitteissa vielä kesken. Kuitenkin voidaan jo tässä vaiheessa, ensimmäisen kehittämissyklin päätyttyä tunnistaa asioita, joiden suunnittelu tällä kehittämistavalla on onnistunutta ja toisaalta asioita jotka näin jälkikäteen tarkasteltuna olisi voitu tehdä toisin.

Poliisin salassa pidettävien tietoaineistojen käsittelymääräyksen valmistelu ja koulutus on saadun palautteen mukaan onnistunut kohtalaisesti. Tietyt tekniset rajoitteet ovat aiheuttaneet henkilöstölle ongelmia, mutta niiden esiintulon jälkeen ongelmiin on puututtu järjestelmiä ja ohjeistusta kehittäen.

Kun lähes kaksi vuotta on kulunut tietoturva-asetuksen mukaisen uuden luokittelumallin käyttöönoton jälkeen, poliisihallinnossa edelleen yksittäisiä väärin tai vanhan normiston mukaan luokiteltuja tai merkittyjä asiakirjoja esiintyy. Yleisten havaintojen mukaan pääsääntöisesti kuitenkin luokitusperusteet ja leimat alkavat olla oikein määritettyjä.

Samaan aikaan luokittelu ja salassapitoleimat on otettu merkittävästi laajempaan käyttöön erityisesti poliisin sisäiseen käyttöön tarkoitettujen asiakirjojen osalta ja henkilöstön ymmärrys eri suojaustasojen käsittelyrajoituksista on huomattu kasvaneen. Henkilöstö myös entistä aktiivisemmin tuo esille mahdollisia tietoteknisiä tai muita käytännön ongelmia tietoaineistojen käsittelyssä, mikä viittaisi että käsittelysäännöt tunnetaan entistä paremmin ja niitä pyritään noudattamaan päivittäisessä työssä.

Kun yleisohjeistus salassa pidettävien tietoaineistojen käsittelyyn on päivitetty ja otettu henkilöstön toimesta käyttöön, on herännyt tarve tarkemmalle ohjeistukselle ja koulutuksen ulottaminen laajemmalle kohdejoukolle kun kehittämisprosessin alussa suunniteltiin. Nämä toimenpiteet on aikataulutettu seuraavaan sykliin.

Tietoturvatasojen kehittäminen suunniteltiin tehtäväksi yksiköiden itsearviointien ja sisäisen kehittämistyön osana. Nykyisten kokemusten ja saadun palautteen perusteella, tietoturvatasojen vaatimusten yleisyys ja yksiköiden tietoturvaresurssien vaihtelevuus aiheutti ongelmia. Tietoturvatasovaatimusten kehittäminen olisi kannattanut suunnitella tarkemmin konsernitasolla keskitettynä ja käyttää yksiköiden resursseja ainoastaan tarkkaan valituissa yksikkökohtaisissa kehittämistoimenpiteissä. Toisaalta näin laajasti toimien yksiköissä tietoturvavaatimusten osaaminen on kasvanut huomattavasti vuodesta 2010. Toimenpiteitä tullaan

konkretisoimaan seuraavassa kehittämissyklissä tarkennetun kehittämissuunnitelman mukaisesti. Tälle kehittämiselle on jatkossa entisestään parempi mahdollisuus kun tietoturvatasotyön pohjatyö on nyt kaikissa poliisin yksiköissä tehty.

Nyt tehty työ on hyvässä aikataulussa ja vaikka perustaso ei aivan kaikilta vaatimuksiltaan itse asetettuna tavoitteena 1.1.2013 täyttyisi, poliisi on nykyisellä tiedolla saavuttamassa sille asetetut tietoturvavaatimukset siirtymäaikojen puitteissa.

Tästä työstä saatuja kokemuksia voidaan hyödyntää myös muissa suurissa valtionhallinnon virastoissa tai hallinnonaloilla tietoturvallisuutta kehitettäessä tai uusia toimintatapoja jalkautettaessa.

Lähteet

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999). Viitattu 2.12.2012.
http://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Eskola, J., Suoranta, J. 2005. Johdatus laadulliseen tutkimukseen. 7. Painos. Jyväskylä: Jyväskylän kirjapaino.

Jyrkämä, J. 1978. Toimintatutkimuksen teoriasta ja tutkimuskäytännöstä. Sosiaalipolitiikka.

Katila, S. & Meriläinen, S. 2006. Henkilökohtainen kokemus tiedon lähteenä: toimintatutkimus akateemisessa yhteisössä. Helsinki: Gaudeamus.

Kolb, D. A. 1984. Experiential learning. Experience as the source of learning and development. Englewood Cliffs N.J. Prentice-Hall

Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (621/1999). Viitattu 2.12.2012.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Poliisihallitus. 2010. Poliisin tietoturvapolitiikka (2020/2010/4157).

Poliisihallitus. 2010. Poliisin tietoturvatasoauditointiraportti.

Poliisihallitus. 2011. Poliisin tietojärjestelmien tietoturvavaatimukset (2020/2011/2531).

Poliisihallitus. 2012. Poliisin tietojärjestelmien käyttöönottopäätös ja järjestelmätietojen hallinta (2020/2012/2751).

Poliisin hallintorakenne. 2012. Viitattu 2.12.2012
http://www.poliisi.fi/poliisi/home.nsf/pages/E9D8E3C4F56C4927C2256B8700455C96?opendocument

Poliisin vuosikertomus 2011. Tulostettu 2.12.2012.
http://www.poliisi.fi/poliisi/home.nsf/ExternalFiles/Vuosikertomus2011_web/$file/VuosikertVuos2011_web.pdf

Sisäasiainministeriö. 2006. Sisäasiainministeriön määräys salassa pidettävien tietoaineistojen luokittelusta ja käsittelystä (SM-2006-02986/Vi-1).

Sisäasiainministeriö. 2008. Poliisihallinnon tietoturvaperiaatteet (SMDno/2008/353).

Tertsunen, T. 1999. Toimintatutkimus tietokoneavusteisten opetusohjelmien hyödynnettävyydestä ammatillisessa koulutuksessa sähköalalla. Viitattu 17.12.2012
http://ethesis.helsinki.fi/julkaisut/kas/kasva/pg/tertsunen/6luku.html

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). Viitattu 25.5.2012.
http://www.finlex.fi/fi/laki/alkup/2010/20100681

Valtiovarainministeriö. 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010). Tampereen Yliopistopaino.

Kuvat

Taulukot

Liitteet

Liite 1: Määräys poliisin salassa pidettävien tietoaineistojen käsittelystä

MÄÄRÄYS POLIISIN SALASSA PIDETTÄVIEN TIETOAINEISTOJEN KÄSITTELYSTÄ

Tämä määräys sisältää salassa pidettävien tietoaineistojen käsittelyssä noudatettavat periaatteet poliisihallinnossa. Määräys perustuu lakiin viran-omaisten toiminnan julkisuudesta (621/1999) sekä 1.10.2010 voimaan tulleeseen Valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010).

Määräyksessä määritellään hyvän tiedonhallintatavan ja tietoturvallisuuden varmistamistarpeiden mukaiset tietojen luokituskäytännöt erityisesti luottamuksellisuuden osalta sekä tähän luokitteluun perustuvien tietojen käsittelyvaatimukset.

Määräys kumoaa Sisäasiainministeriön määräyksen Poliisihallinnon tietoturvaperiaatteet SMDno/2008/353 kappaleiden Tietoaineistoturvallisuus, Tietoaineiston määritelmä sekä yhdistelmä salassa pidettävän tietoaineiston käsittelystä poliisissa osalta (sivut 19-23).

1 Johdanto

1.1 Tarkoitus ja soveltamisala

Määräyksessä määritellään salassa pidettävien tietoaineistojen käsittelyssä noudatettavat periaatteet poliisihallinnossa. Määräys sisältää linjaukset asiakirjojen ja niiden sisältämien tietojen luokituksesta sekä tähän luokitteluun perustuvat käsittelyvaatimukset asiakirjojen elinkaaren eri vaiheiden aikana. Yhtenäisillä menettelyillä luodaan turvalliset tietojen käsittelyn edellytykset poliisihallintoon sekä poliisin lukuun toimivien tietopalvelutoimittajien ja viranomaistietoa käsittelevien osapuolten kanssa.

Määräyksen laatimisessa on otettu huomioon sisäasiainhallinnon voimassa oleva ohjeistus sekä Valtiovarainministeriön Ohje tietoturvallisuudesta annetun asetuksen täytäntöönpanosta (VAHTI 2/2010). VAHTI 2/2010 ohjetta voidaan noudattaa tarkentavana asiakirjana mikäli tässä määräyksessä tai tarkentavissa poliisihallinnon ohjeissa ei asiaa ole ohjeistettu.

Kansainväliseen yhteistyöhön liittyviä (esim. EU, NATO, EUROPOL, INTERPOL) asiakirjoja käsittelevien tulee ottaa huomioon niiden käsittelyn mahdolliset erityispiirteet, jotka liittyvät niiden jakeluun ja suojaamiseen.

1.2 Lainsäädäntö ja kansainväliset velvoitteet

Salassa pidettävän tietoaineiston käsittelyssä on noudatettava erityistä huolellisuutta. Tätä koskevat velvoitteet sisältyvät lakiin viranomaisten toiminnan julkisuudesta (621/1999) (julkisuuslaki) ja valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010) (tietoturva-asetus). Virkamiehen ja julkisyhteisön työntekijän salassapitovelvollisuuden rikkomisesta ja muiden henkilöiden salassapitorikoksesta ja rikkomuksesta säädetään rikoslaissa.

Julkisuuslain mukaan viranomaisen asiakirjat ovat julkisia, jollei lailla toisin säädetä. Asiakirjan käsite on julkisuuslaissa laaja ja se kattaa myös erilaiset tekniset tallenteet. Laissa on erikseen määritelty ne asiakirjat, jotka ovat joko kokonaan tai osittain salassa pidettäviä. Salassapitovelvollisuudesta on säännöksiä myös muissa laeissa. Tuomioistuimet voivat myös lain nojalla määrätä asiakirjan salassa pidettäväksi.

Henkilötietojen käsittelyä koskevat yleissäännökset sisältyvät henkilötieto-lakiin (523/1999). Viranomaisten henkilörekistereiden julkisuutta ja salassapitoa arvioidaan kuitenkin julkisuuslain ja mahdollisten erityislakien mukaisesti.

On huomattava, että sellaisiin muistiinpanoihin ja luonnoksiin, jotka muutoin jäävät julkisuuslain mukaan viranomaisen asiakirjan käsitteen ulkopuolelle, sovelletaan kuitenkin lain salassapitosäännöksiä. Salassapitosäännöksiä sovelletaan myös asiakirjoihin jotka liittyvät yksityisen lukuun suoritettavaan tehtävään.

Julkisuuslain mukaan jokaisen asiakirjan julkisuus on selvitettävä tapaus-kohtaisesti silloin, kun joku pyytää asiakirjaa nähtäväkseen tai saadakseen siitä kopion. Asiakirjarekisteriin, esimerkiksi diaariin, merkittyjen tietojen julkisuutta on arvioitava erillään asiakirjojen julkisuudesta.

Salassapitoa ei saa ulottaa laajemmalle kuin suojattava etu vaatii. Jos asiakirjasta vain osa on salassa pidettävää, viranomaisen on annettava asiakirjasta tieto muilta osin. Viranomaisen on julkisuuslaissa asetetussa määräajassa tehtävä päätös kieltäytyessään antamasta tietoa asiakirjasta. Viranomaisen on perusteltava huolellisesti päätös tiedonsaannin epäämiselle.

Tietoa salassa pidettävän asiakirjan sisällöstä saa lain mukaan antaa vain viranomainen tai se virkamies, jolle tällainen oikeus on nimenomaisesti työ-järjestyksessä tai vastaavalla tavalla annettu. Salassa pidettävän tiedon luovuttaminen ilman asianmukaista oikeutta on rangaistavaa.

Tietoturvallisuuden varmistamiseksi tehtävä asiakirjojen luokittelu ja sitä vastaavien merkintöjen tekeminen asiakirjaan ei muuta edellä kuvattua velvollisuutta arvioida asiakirjan julkisuus erikseen ja tapauskohtaiseksi silloin, kun viranomaiselta pyydetään asiakirjaa. Ainoa poikkeus tästä säännöstä ovat asiakirjat, joihin on tehty turvallisuusluokitusmerkintä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisesti.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisalan piiriin kuuluvien asiakirjojen käsittelyssä noudatetaan Suomea sitovia kansainvälisiä määräyksiä, jotka perustuvat joko kahden- tai monenvälisiin sopimuksiin tai EU-säädöksiin.

1.3 Määräyksen keskeisimmät käsitteet

Asiakirja: Kirjallisen ja kuvallisen esityksen lisäksi sellainen käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuva tiettyä kohdetta tai asiaa koskeva viesti, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apu-välineiden avulla. (Julkisuuslaki 5.1 §)

Asiakirjan käsite on riippumaton siitä, minkälaiselle alustalle tai minkälaisin keinoin tieto on talletettu. Siten asiakirjoilla tarkoitetaan paitsi perinteisiä paperimuotoisia asiakirjoja, myös sähköisesti talletettuja tietoaineistoja riippumatta niiden muodosta.

Viranomaisen asiakirja: Viranomaisen hallussa oleva asiakirja, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. Viranomaisen laatimana pidetään myös asiakirjaa, joka on laadittu viranomaisen antaman toimeksiannon johdosta. Viranomaiselle toimitettuna asiakirjana pidetään asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten (Julkisuuslaki 5.2 §; käsitteen ulkopuolelle jäävistä asiakirjoista, ks. em. lain 5.3 ja 5.4 §).

Tietoaineisto: Paperilla, sähköisillä tai muilla tietovälineillä oleva asiakirja ja tieto. Asiakirjalla tarkoitetaan viranomaisen toiminnan julkisuudesta annetussa laissa määriteltyjä asiakirjoja.

Asiakirjan haltija: Se organisaatio tai henkilö, jonka hallussa asiakirja on.

Asiakirjan laatija: Se organisaatio tai henkilö, joka on laatinut asiakirjan.

Etäkäyttö: Poliisin tai hallinnonalan tietoteknisessä ympäristössä olevien palveluiden käyttö verkon ulkopuolelta.

Henkilötieto: Kaikenlaiset luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. (HetL 3.1 § 1 kohta)

Arkaluonteinen henkilötieto: Henkilötieto, joka kuvaa tai on tarkoitettu kuvaamaan (HetL 11 §):

1) rotua tai etnistä alkuperää;
2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Henkilötietojen käsittely: Henkilötietojen kerääminen, tallettaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen sekä muut henkilö-tietoihin kohdistuvat toimenpiteet. (HetL 3.1 § 2 kohta)

Henkilörekisteri: Käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojoukko, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta (ns. looginen rekisterikäsite). (HetL 3.1 § 3 kohta)

Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.

Tietoturvatasot: Tietoturvatasoilla (tai tietoturvallisuustasoilla) tarkoitetaan niitä teknisiä ja hallinnollisia järjestelyjä, joiden avulla varmistetaan tietoturvallisuuden toteuttaminen eri suojaustasoilla. Perustason vaatimukset täyttävässä ympäristössä voidaan toteuttaa suurin osa viranomaisen tiedonkäsittelytarpeista. Niiden asiakirjojen käsittelyssä, jossa edellytetään korkeaa luotettavuutta kaikissa toimintaolosuhteissa ja jossa käsitellään suojaustasoa III edellyttävää luokiteltua aineistoa, viranomaisen on ylläpidettävä korotetun tietoturvatason täyttäviä rakenteita. Kriittiset ja suojaustasoille I ja II luokiteltua tietoa sisältävät tietojärjestelmät tulee toteuttaa korkean tieto-turvatason ympäristöissä.

Salassa pidettävä asiakirja: Salassa pidettävällä asiakirjalla tarkoitetaan niitä asiakirjoja ja tietoja, jotka ovat julkisuuslain 24.1 §:n tai muun lain nojalla salassa pidettäviä. Asiakirjaa tulee käsitellä suojaustason mukaisesti ja siihen tulee tehdä suojaustason mukainen merkintä. Lisäksi osa salassa pidettävistä asiakirjoista määritellään ja merkitään turvallisuusluokituksen mukaisesti (katso kohta turvallisuusluokiteltava asiakirja).

Luokiteltu asiakirja: Suojaustaso- tai turvallisuusluokiteltua tietoa sisältävä asiakirja. Salassa pidettävän tietoaineiston suojaustasoluokka määritellään sen mukaan, kuinka vakavia seurauksia tietojen oikeudettomasta paljastumisesta tai käytöstä seuraisi suojattaville eduille.

Suojaustasot: Suojaustasojen avulla määritellään vaatimukset, jotka tietojenkäsittely-ympäristön ja tietojen käsittelyn tulee täyttää käsiteltäessä luokiteltavaa asiakirjaa. Suojaustasot toteutetaan neliportaisen luokitusjärjestelmän avulla. Kullekin suojaustasolle on asetettu omat tekniset ja toiminnalliset vaatimukset. Näiden menettelyjen avulla turvataan salassa pidettävän ja muun luokittelua edellyttävän tiedon asianmukainen käsittely (tieto-

turvallisuusasetus, 9 §). Tietojen käsittely tapahtuu suojaustason mukaisesti riippumatta siitä onko kysymyksessä suojaustaso- vai turvallisuus-luokiteltu tieto.

Turvallisuusluokiteltava asiakirja: Salassa pidettävää tietoaineistoa sisältävä asiakirja, jonka tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maan-puolustukselle tai muille yleisille eduille julkisuuslain 24 §:n 1 momentin 2, 7 – 10 kohdissa tarkoitetulla tavalla tai asiakirja, jonka luokittelu on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liittyy kansainväliseen yhteistyöhön. Näiden asiakirjojen käsittelyssä on noudatettava luokkaa vastaavia tietoturvavaatimuksia.

2 Tietoaineistojen luokitteluvaatimukset

2.1 Luokittelun perusteet

Julkisuuslaki asettaa viranomaiselle velvoitteet hallita käytössään olevia tietoaineistoja hyvän tiedonhallintatavan mukaisesti. Tietoaineistojen hallinnan apuna käytetään muun muassa arkistonmuodostussuunnitelmaa ja tarvittavia rekistereitä ja luetteloja. Tietoaineistojen käytettävyyttä, eheyttä ja luottamuksellisuutta hallitaan luokittelemalla aineisto eri luokkiin tiedolle asetettujen toiminnallisten vaatimusten pohjalta.

Viranomaisten tietoaineistot ovat julkisia, jollei toisin säädetä.

Julkisuuslainsäädännön ja salassapitosäännösten pohjalta määritetään onko tietoaineiston sisältämä tieto julkista vai salassa pidettävää. Salassa pidettävien tietoaineistojen käsittelyä ohjataan suojaustasoluokkien avulla (Kuva 1, Suojaustasomerkintä). Salassa pidettäviä tietoaineistoja käsitellään kyseistä tietoa vastaavan suojaustason edellyttämällä tavalla.

Salassa pidettävän tietoaineiston suojaustasoluokka määritellään sen mukaan, kuinka vakavia seurauksia tietojen oikeudettomasta paljastumisesta tai käytöstä seuraisi suojattaville eduille. Kukin tietoaineisto ja sen oikeudettomasta paljastumisesta tai käytöstä aiheutuvat seuraukset on arvioitava konkreettisesti ja ottaen huomioon suojattava etu kokonaisuutena. Luokitusta ei saa ulottaa sellaiseen asiakirjaan tai asiakirjan osiin, joissa käsittelyvaatimusten noudattaminen ei suojattavan edun vuoksi ole tarpeen.

Tietoturva-asetuksessa on määritelty ne muut asiakirjat, jotka voidaan luokitella suojaustasoa IV edellyttäväksi asiakirjaksi. Tällaisia ovat vain sellaiset asiakirjat ja niihin sisältyvät tiedot, joiden luovuttaminen on lain mukaan viranomaisen harkinnassa (esim. harkinnanvaraisesti julkiset asiakirjat) tai joita saadaan lain mukaan luovuttaa vain määrättyyn tarkoitukseen

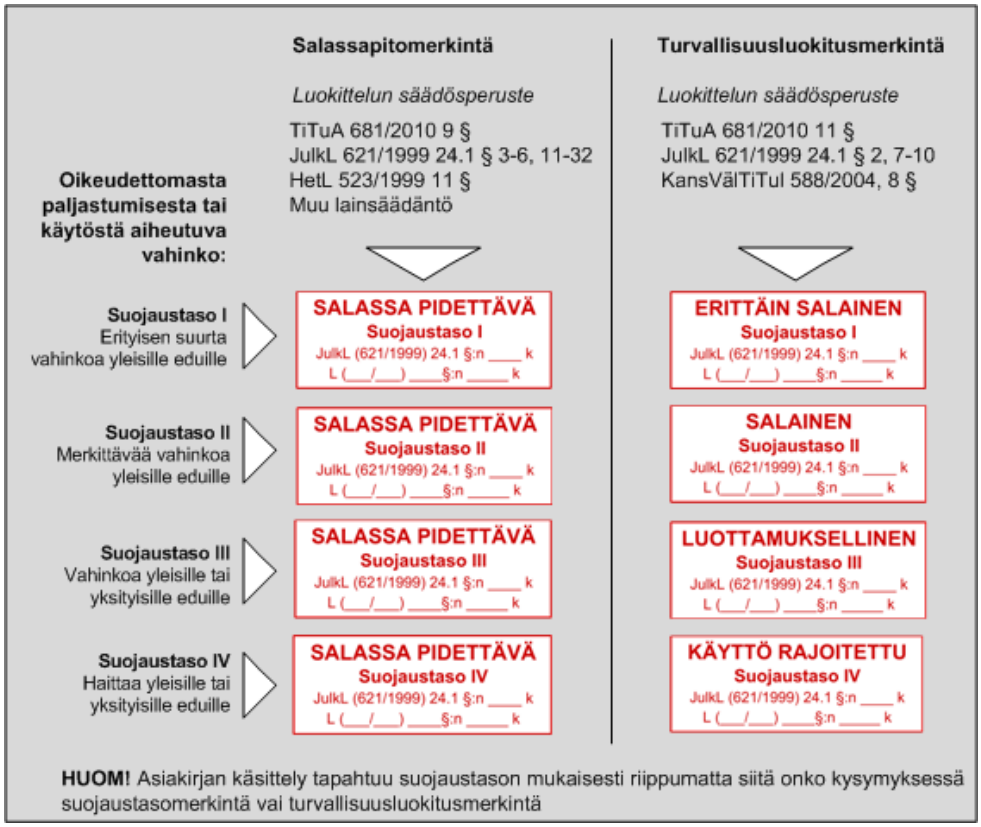
(esim. henkilörekisterit). Lisäksi tiedon oikeudettoman paljastumisen tulee voida aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Luokittelu voidaan tehdä myös siten, että tietoturvallisuutta koskevat vaatimukset kohdistetaan vain sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen.

Salassapidon arviointi tulee tehdä jo asiakirjaa laadittaessa. Luokitusmerkinnän tekemisestä asiakirjaan päättää asiakirjan allekirjoittaja tai työjärjestyksessä erikseen määrätty henkilö. Luokitusmerkintä kertoo laatijan ja allekirjoittajan käsityksen siitä, millä tavalla asiakirja on suojattava ja kenelle asiakirja on tarkoitettu (jakelu). Luokitusmerkinnästä riippumatta salassa pidettävää tietoa ei saa luovuttaa sen hallussa pitämiseen oikeutettujen ulkopuolelle.

Asiakirjan sisältämän salassa pidettävän tiedon paljastaminen sivullisille ei ole sallittua, vaikka asiakirjaan ei olisi merkitty suojaustasoa.

Sellainen salassa pidettävä tietoaineisto, jonka tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille julkisuuslain 24 §:n 1 momentin 2, 7 – 10 kohdissa tarkoitetulla tavalla, on turvallisuus-luokiteltava (Kuva 1, Turvallisuusluokitusmerkintä).



Kuva 1, salassa pidettävien asiakirjojen luokittelu ja niiden merkitseminen.

Koska ilmaisu ”LUOTTAMUKSELLINEN” on tietoturva-asetuksessa tarkoitettu turvallisuusluokka, asiakirjaan ei ole lainmukaista tehdä tätä vastaavaa merkintää muulloin, kuin kysymyksen todella ollessa kyseiseen turvallisuusluokkaan kuuluvasta asiakirjasta.

2.2 Salassapitomerkinnät

Viranomaisen on tehtävä salassapitomerkintä viranomaisen asiakirjaan, jonka se antaa asianosaiselle ja joka on salassa pidettävä toisen tai yleisen edun vuoksi. Merkintä voidaan tehdä muihinkin salassa pidettäviin asiakirjoihin. Suositeltavaa on, että merkintä tehdään myös annettaessa salassa pidettävä asiakirja toiselle viranomaiselle tai sille, joka viranomaisen toimeksiannon perusteella käsittelee salassa pidettäviä tietoja.

Pääsääntöisesti salassapitomerkintä tehdään asiakirjan ensimmäiselle sivulle sivun oikeaan yläkulmaan. Suojaustasojen I ja II asiakirjoissa voidaan punaisen salassapitomerkintäleiman lisäksi käyttää punaista poikkiviivaa jokaisella sivulla.

Merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu. Salassapitovelvollisuus ilmaistaan joko osoittamalla ne osat asiakirjasta, jotka ovat salassa pidettäviä (esim. liitteen jakso 1.2.) tai ilmaisemalla, minkälaiset tiedot ovat salassa pidettäviä (esim. hakijan terveydentilaa koskevat tiedot). Merkinnästä tulee käydä ilmi myös mille suojaustasolle tietoaineisto luokitellaan (kappaleet 2.3 ja 2.4).

Asiakokonaisuuksia lähetettäessä tulee kokoavassa tai lähetyksen ensimmäisessä asiakirjassa olla merkintä asian salassa pidettävyydestä perus-teineen sekä viittaus mitä osaa asiakokonaisuudesta salassapitovaatimus koskee. Tämä vaatimus ei poista itse salassa pidettävän asiakirjan merkintävaatimusta.

Turvallisuusluokiteltava aineisto merkittään määräyksen mukaisilla leimoilla ja merkinnöillä koko asiakirjan elinkaaren ajan aina siihen asti, kun tietoon sisältyy salassapitovaatimus. Turvallisuusluokittelua edellyttävä aineistoa luovutettaessa on varmistuttava että luovutukseen on olemassa oikeus ja tarve ja että luovuttaja täyttää tietoaineiston käsittelyltä vaadittavat edellytykset.

2.3 Suojaustasot ja merkinnät

SALASSA PIDETTÄVÄ, suojaustasot I-IV.

Leimaan kirjoitetaan käsin tai koneellisesti suojaustasoa osoittava numero. Salassa pidettävä leimaa käytetään asiakirjoissa, jotka sisältävät joko julkisuuslain 24.1 §:n kohdissa 1, 3 - 6 sekä 11 - 32 tai muussa laissa määriteltyä salassa pidettävää tietoa.

Tämän lisäksi leimaa voidaan käyttää suojaustasolla IV asiakirjoihin, joiden luovuttaminen on viranomaisen harkinnassa (esim. harkinnanvaraisesti julkiset asiakirjat) tai joita saadaan lain mukaan luovuttaa vain määrättyyn tarkoitukseen (esim. henkilörekisterit) ja tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Suojaustasot ovat:

- **suojaustaso I (ST I)**, jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa salassapito-säännöksessä tarkoitetuille yleisille eduille;

- **suojaustaso II (ST II)**, jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille;

- **suojaustaso III (ST III)**, jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleisille tai yksityisille eduille ja oikeuksille;

- **suojaustaso IV (ST IV)**, jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleisille tai yksityisille eduille tai, jos tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

SALASSA PIDETTÄVÄ

Suojaustaso __

JulkL (621/1999) 24.1 §:n _____k

Luokitusmerkintä voidaan jättää tekemättä, jos kaikki asiakirjaa viranomaisessa käsittelevät ovat tietoisia asiakirjan salassapidosta ja sen käsittelyssä noudatettavista menettelytavoista. Esimerkiksi tietojärjestelmissä, joissa erikseen valtuutetut henkilöt käsittelevät pelkästään henkilörekisterien piiriin kuuluvia henkilötietoja, ei edellytetä tässä määräyksessä mainittujen merkintöjen käyttämistä normaaleissa käsittelytilanteissa. Tietoja käsittelevien tulee kuitenkin tunnistaa näiden asiakirjojen ja tietojen käsittelyyn sisältyvät käyttörajoitusehdot.

Asiakirjaan tehtävä luokitusmerkintä voidaan jättää tekemättä myös silloin, kun salassapitovelvollisuus ja siitä johtuvat käsittelyvaatimukset ovat voi-massa vain suhteellisen lyhyen ajan tai silloin, kun asiakirjassa on vain joitakin salassapitovelvollisuuden piiriin kuuluvia tietoja ja joissa kaikki asiakirjaa käsittelevät ovat tietoisia sen luonteesta. Näissä tapauksissa on asianmukaisempaa, että salassapitoa ja käsittelyvaatimuksia koskevat tiedot merkitään erilliseen asiakirjan yhteydessä säilytettävään asiakirjaan.

Tiedon salassa pitäminen lakkaa kun asiakirjan laatimisesta on kulunut laissa säädetty tai sen nojalla määrätty aika. Mikäli salassa pidettävä tieto on sellainen, että tarve salassa pitämiseen määrätyn ajan kuluttua lakkaa, tulee tuo määräaika asiakirjan laatijan tai haltijan toimesta ilmoittaa asiakirjassa tai erillisenä kirjallisena tai sähköisenä tietona. Mikäli asiakirjassa on luokitusmerkintä, on tarkoituksenmukaista merkitä salassa pidon lakkaaminen luokitusmerkinnän yhteyteen.

2.4 Turvallisuusluokat ja merkinnät

Tietoaineisto voidaan turvallisuusluokitella tietoturva-asetuksessa osoite-tuissa tapauksissa neljään turvallisuusluokkaan (TL). Turvallisuusluokiteltua aineistoa käsitellään suojaustasoluokille annettujen vaatimusten mukaisesti.

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin julkisuuslain 24 § 1 momentin 2,7 – 10 kohtiin tarkoitetuissa tapauksissa ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.

Turvallisuusluokat ovat:

Turvallisuusluokka I (ERITTÄIN SALAINEN), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille;

ERITTÄIN SALAINEN

Suojaustaso I

JulkL (621/1999) 24.1 §:n k

Turvallisuusluokka II (SALAINEN), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa merkittävää vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille;

SALAINEN

Suojaustaso II

JulkL (621/1999) 24.1 §:n _____k

Turvallisuusluokka III (LUOTTAMUKSELLINEN), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansain-välisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille;

LUOTTAMUKSELLINEN

Suojaustaso III

JulkL (621/1999) 24.1 §:n _____k

Turvallisuusluokka IV (KÄYTTÖ RAJOITETTU), jos salassa pidettävän tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa haittaa julkisuus-lain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille.

KÄYTTÖ RAJOITETTU

Suojaustaso IV

JulkL (621/1999) 24.1 §:n _____k

Turvallisuusluokkien merkinnät on esitetty oheisessa taulukossa.

TURVALLISUUSLUOKKA	NIMIKE	LYHENNE
Turvallisuusluokka I	ERITTÄIN SALAINEN	ERSAL (E)
Turvallisuusluokka II	SALAINEN	SAL (S)
Turvallisuusluokka III	LUOTTAMUKSELLINEN	LUOT (L)
Turvallisuusluokka IV	KÄYTTÖ RAJOITETTU	RAJ (R)

Lyhenteitä voidaan käyttää tietojärjestelmissä ja asiakirjoissa soveltuvin osin.

Ruotsiksi käännetyissä tai ruotsiksi laaduissa turvallisuusluokitelluissa asiakirjoissa merkintä tulee tehdä ruotsiksi. Vastaavat merkinnät on kuvattu alla.

TURVALLISUUSLUOKKA	**NIMIKE SUOMEKSI**	**NIMIKE RUOTSIKSI**
Turvallisuusluokka I	ERITTÄIN SALAINEN	YTTERST HEMLIG
Turvallisuusluokka II	SALAINEN	HEMLIG
Turvallisuusluokka III	LUOTTAMUKSELLINEN	KONFIDENTIELL
Turvallisuusluokka IV	KÄYTTÖ RAJOITETTU	BEGRÄNSAD TILLGÅNG

2.5 Kansainvälisten aineistojen turvallisuusluokat

Kansainvälisiltä järjestöiltä ja toisilta valtioilta tulleissa asiakirjoissa voi olla järjestöjen ja valtioiden omia luokitusmerkintöjä. Niihin tehdään Suomen vastaavaa turvallisuusluokkaa koskeva merkintä, jos turvallisuusluokiteltujen tietojen molemminpuolisesta suojelusta on tehty Suomea sitova sopimus tai asiakirja muutoin kuuluu kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisalan piiriin (esim. EU:n komission tai neuvoston turvallisuusluokittelema asiakirja).

Jos vieraan valtion tai kansainvälisen järjestön kanssa ei ole sitovaa sopimusta tai asiakirjaa turvallisuusluokkia koskevista järjestelyistä, tulee viranomaisen päättää merkinnän tekemisestä Suomen lainsäädännön mukaan.

Alla olevasta taulukosta ilmenee eräiden kansainvälisten järjestöjen ja Suomen turvallisuusluokituksien vastaavuus.

Kohde	Turvallisuusluokka I	Turvallisuusluokka II	Turvallisuusluokka III	Turvallisuusluokka IV
Suomi	ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUK-SELLINEN	KÄYTTÖ RAJOITETTU
EU	TRÉS SECRET UE/ EU TOP SECRET	SECRET UE/ EU SECRET	CONFIDENTIEL UE/ EU CONFIDENTIAL	RESTREINT UE/ EU RESTRICTED
NATO	COSMIC TOP SE-CRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
EUROPOL	EUROPOL TOP SE-CRET	EUROPOL SECRET	EUROPOL CONFIDEN-TAL	EUROPOL RESTRICTED

EU:n sisäiset asiakirjat, jotka on merkitty "LIMITE" merkinnällä, tarkoittaa näiden jakelun rajoittamista eikä ole turvallisuusluokkaa ilmaiseva merkintä. Merkitsemällä asiakirjan tällä merkinnällä on lähettäjä tarkoittanut, että tätä ei jaeta julkisuuteen. Sama koskee NATO UNCLASSIFIED asiakirjoja. Kummankin asiakirjaryhmän luokitus Suomessa on arvioitava tapauskohtaisesti kansallisen lainsäädännön mukaan.

2.6 Henkilötietojen luokitus ja merkinnät

Henkilötietojen käsittelyä ja henkilörekistereitä ohjaavat julkisuuslain lisäksi henkilötietolaki, laki henkilötietojen käsittelystä poliisitoimessa (761/2003) ja useat eri henkilötietojen käsittelyä koskevat erityislait, jotka asettavat erityisvaatimuksia mm. arkaluonteisten tietojen käsittelylle ja tietojen suojaamiselle. Käyttötarkoitussidonnaisuus ja luovutusperusteet asettavat omia vaatimuksiaan henkilötietojen käsittelylle.

Poliisin henkilörekistereiden ja niihin sisältyvien tietojen julkisuus- ja salassapitoperusteet sekä luokitusta koskevat vaatimukset ovat samoja kuin muissakin asiakirjoissa.

Mikäli salassa pidettävän asiakirjan sisällöstä ei muuta johdu, arkaluonteisia henkilötietoja sisältävät asiakirjat luokitellaan suojaustasolle III.

Muita kuin arkaluonteisia henkilötietoja sisältävät asiakirjat luokitellaan suojaustasolle IV, mikäli se on suojattavan edun vuoksi tarpeen. Myös henkilötietoja sisältäviä luokittelemattomia asiakirjoja käsitellään lähtökohtaisesti suojaustason IV mukaisesti.

Henkilötunnuksen sisältäviä asiakirjoja on käsiteltävä suojaustason IV mukaisesti, ellei asiakirjan sisällön perusteella asiakirjaa kuulu käsitellä korkeamman suojaustason vaatimusten mukaisesti.

3 Tietoaineistojen käsittelyvaatimukset

3.1 Tietoaineiston hallussapito- ja käsittelyoikeudet

I ja II suojaustason tietoaineistoa saavat käsitellä vain vastaanottajaksi merkityt ja henkilöt, jotka ovat siihen oikeutettuja sekä henkilöt, jotka ovat oikeutettuja tällaisen tietoaineiston tekniseen (vastaanotto, arkistointi yms.) hallussapitoon ja käsittelyyn vastaanottavassa virastossa tai laitoksessa.

Suojaustasoon I ja II luokiteltujen tietoaineistojen käyttöoikeus voidaan antaa ainoastaan henkilöille, joilla työtehtäviensä vuoksi on tarve saada tietoja tietoaineistosta tai muutoin käsitellä sitä ja joka tuntee aineiston käsittelyä koskevat velvoitteet.

Poliisin yksiköiden on pidettävä luetteloa niistä työtehtävistä, joissa on oikeus käsitellä suojaustasoa I tai II edellyttäviä asiakirjoja. Työtehtäväluettelot tulee tarkistaa ja saattaa ajan

tasalle vähintään kerran vuodessa. Ajan-tasaiset luettelot toimitetaan tiedoksi poliisin tietoturvapäällikölle.

III ja IV suojaustasojen tietoaineistoja voivat pitää hallussaan ja käsitellä kaikki poliisihallinnon virkamiehet ja työntekijät heidän työtehtäviensä mukaisissa asioissa.

3.2 Tietoaineiston käsittely, tallennus tietovälineille sekä kopiointi ja tulostus

I suojaustason tietoaineiston käsittelyä varten on varattava erilliset vain tätä tarkoitusta varten tarkoitetut laitteet, jotka ovat erillään tietoverkoista ja täyttävät korkean tietoturvatason vaatimukset.

I ja II suojaustasoon luokiteltavia tietoaineistoja voidaan käsitellä tiloissa joissa pääsy on rajattu vain tunnistetuille henkilöille.

I ja II suojaustasoon luokitellun tietoaineiston saa tallentaa tietovälineelle ainoastaan silloin kun kyseinen tieto tai koko tietovälineen sisältö on vahvasti salattu.

I ja II suojaustasoon luokitellut aineistot tulostetaan laitekohtaisella oheistulostimella. Tulostetut aineistot tulee numeroida. Numeroitujen aineistojen jakelu tulee merkitä alkuperäiseen asiakirjaan tai erilliseen tätä varten laadittuun jakoluetteloon.

II suojaustasoon luokiteltua tietoaineistoa saa käsitellä tietoverkoista erillään olevilla laitteilla tai tietovälineillä tai hallinnonalan tietoverkossa sijaitsevissa tietojärjestelmissä. Tietojärjestelmien on täytettävä korkean tieto-turvatason vaatimukset.

III ja IV suojaustasojen tietoaineistoa saa käsitellä ja tallentaa tietoverkkoon kytketyllä korotetun tietoturvatason vaatimukset täyttävillä tietojärjestelmillä. Tietoaineistoa saa myös tulostaa verkkotulostimella sillä edellytyksellä, että tulostettu asiakirja noudetaan välittömästi tulostimelta. III ja IV suojaus-tasojen aineistot on tallennettava tietojärjestelmiin, levyalueille tai erillisille tietovälineille siten, että tietoa voivat käsitellä vain siihen oikeutetut henkilöt.

Salassa pidettävien tietoaineistojen tallennus siirrettäville tietovälineille tulee tehdä aina vahvasti salattuna.

Pääsy tulee rajata vain tunnistettaviin henkilöihin myös arkistoissa, tietokonesaleissa tai muissa tietojärjestelmien ylläpidon tai tietoliikenteen toimivuuden kannalta merkityksellisissä

tiloissa, joissa säilytetään tai käsitellään suojaustasoon III kuuluvia asiakirjoja tai suojaustasoon IV kuuluvia valta-kunnalliseen henkilörekisteriin talletettuja asiakirjoja.

3.3 Tietoaineiston säilytys

I suojaustason asiakirjat kirjataan aina omaan erittäin salaisten asioiden di-aariin. II suojaustason asiakirjat kirjataan aina salaisten asioiden diaariin. Suojaustason I ja II paperimuotoiset asiakirjat ja niiden luonnokset ml. niitä sisältävät tietovälineet on säilytettävä ja arkistoitava holvissa tai murtosuojatussa säilytyskaapissa tai vastaavassa. I ja II suojaustason tietoaineistoja sisältäville arkistoille on määrättävä omat vastuulliset hoitajansa.

Suojaustasoon III ja IV kuuluvat asiakirjat kirjataan julkisten asioiden diaariin käyttäen samaa juoksevaa numeroa siten että tietoihin ja asiakirjoihin on rajattu pääsy. III ja IV suojaustasojen tietoaineistojen diaaritiedot tai otsikoinnit on laadittava siten, etteivät ne itsessään sisällä III tai IV suojaus-tason tietoa. Diaaritiedoista tulee käydä ilmi tietoaineiston suojaustaso. III-IV suojaustasoon kuuluvista tietoaineistojen laatimisesta, lähettämisestä ja vastaanottamisesta on pidettävä luetteloa myös sellaisissa toimipisteissä, joissa ei ole muodostettu omaa diaaria. Suojaustasojen III ja IV paperisia asiakirjoja tulee säilyttää lukitussa kaapissa tai vastaavassa.

3.4 Tietoaineiston kuljettaminen virkapaikan ulkopuolelle

I suojaustason tietoaineistoa, tai niitä sisältäviä tietovälineitä, ei saa viedä virkapaikan ulkopuolelle ilman yksikön päällikön erillistä päätöstä. Päätöksistä pitää kirjaa yksikön tietoturvapäällikkö- tai vastaava.

II suojaustason tietoaineistoa, tai niitä sisältäviä tietovälineitä, saa kuljettaa virkapaikan ulkopuolelle niiden käsittelyyn oikeutettu henkilö vain välttämättömiin työtehtäviin liittyen. II suojaustason paperisten tai laajojen sähköisten tietoaineistojen kuljettamiseen virkapaikan ulkopuolelle tulee olla yksikön päällikön erillinen päätös. Päätöksistä pitää kirjaa yksikön tietoturva-päällikkö- tai vastaava. Tietovälineelle tallennetun tietoaineiston kuljettaminen virkapaikan ulkopuolelle on sallittua vain, jos tallennettu tietoaineisto on vahvasti salattu.

III ja IV suojaustasoon kuuluvaa tietoaineistoa saa kuljettaa virkapaikan ulkopuolelle työtehtäviin liittyen. Tietovälineelle tallennetun tietoaineiston kuljettaminen virkapaikan ulkopuolelle on sallittua vain, jos tallennettu tietoaineisto on vahvasti salattu.

3.5 Tietoaineiston käsittely poliisin toimipisteiden ulkopuolella

Poliisin toimipisteiden ulkopuolella ei saa käsitellä suojaustasoon I ja II kuuluvia tietoaineistoja. Poikkeuksen vaatimukseen muodostavat sisäasiain-hallinnon sekä muiden turvallisuusviranomaisten tilat jotka on luokiteltu tietoaineiston suojaustason mukaisesti.

Lisäksi välttämättömissä työtehtävissä ja yksikön päällikön erillisellä päätöksellä voidaan suojaustasoon II kuuluvia tietoaineistoja käsitellä poliisin toimitilojen ulkopuolella. Päätöksistä pitää kirjaa yksikön tietoturvapäällikkö- tai -vastaava. Tällöin tulee huomioida velvoitteet salassa pidettävän tiedon käsittelystä ja suojaamattomasta ympäristöstä aiheutuvat erityiset riskit kuten salakuuntelun tai -katselun mahdollisuus.

Poliisin tai hallinnonalan tietotekniseen ympäristöön tallennettujen I ja II suojaustasoihin kuuluvien tietoaineistojen etäkäyttö on kielletty.

Suojaustasoon III ja IV kuuluvien tietoaineistojen käsittely poliisin toimipisteiden ulkopuolella on mahdollista työtehtäviin liittyen. Tällöin tulee huomioida velvoitteet salassa pidettävän tiedon käsittelystä ja suojaamattomasta ympäristöstä aiheutuvat erityiset riskit kuten salakuuntelun tai -katselun mahdollisuus.

Neuvottelutiloista ja vastaavista on poistettava salassa pidettävää tietoaineistoa sisältävät materiaalit ja piirrokset viimeistään tilaisuuden päätyttyä.

3.6 Tietoaineiston toimittaminen vastaanottajalle

I suojaustason tietoaineiston vastaanottajana on aina henkilö. I suojaus-tasoon kuuluvaa tietoaineistoa voidaan lähettää vain kuriirin välityksellä ja tiedon vastaanottaminen tulee aina varmentaa. Aineistoa ei saa missään tapauksessa lähettää sähköisissä tietoverkoissa.

I suojaustasoon kuuluva lähetettävä tietoaineisto pakataan sinetöityyn, mustaan läpinäkymättömään kirjekuoreen ja sen jälkeen tavalliseen kirje-kuoreen. Mustan kirjekuoren sijasta voidaan käyttää myös tähän tarkoitukseen valmistettua tietoaineistopussia.

II suojaustason tietoaineiston vastaanottaja voi olla henkilö tai organisaatio. II suojaustason aineistoa saa lähettää vastaanottajalle vahvasti salattuna sähköisen tietojärjestelmän tai -verkon välityksellä. Mikäli sähköisessä muodossa olevaa II suojaustason tietoaineistoa lähetetään manuaalisesti (esim. postin tai kuriirin välityksellä), tulee aineisto lähettää tallennettuna käyttämättömälle tietovälineelle ja vahvasti salattuna.

II suojaustasoon kuuluva paperimuotoinen tietoaineisto voidaan lähettää kirjattuna kirjeenä. Postittamisessa tulee välttää perjantaita tai juhla- tai vapaapäivien aattoja. II suojaustasoon

kuuluva lähetettävä tietoaineisto pakataan sinetöityyn, mustaan läpinäkymättömään kirjekuoreen ja sen jälkeen tavalliseen kirjekuoreen. Mustan kirjekuoren sijasta voidaan käyttää myös tähän tarkoitukseen valmistettua tietoaineistopussia.

III suojaustason tietoaineiston vastaanottaja voi olla henkilö tai organisaatio. III suojaustason aineistoa saa lähettää vastaanottajalle vahvasti salattuna sähköisen tietojärjestelmän tai -verkon välityksellä.

III suojaustason tietoaineisto voidaan lisäksi lähettää vastaanottajalle manuaalilähetyksenä. Sähköisessä muodossa tallennetut manuaalilähetykset on vahvasti salattava. III suojaustasoon kuuluva tietoaineisto tulee lähettää läpinäkymättömässä kirjekuoressa. III suojaustasoon kuuluva tietoaineisto suositellaan lähetettäväksi kirjattuna kirjeenä.

IV suojaustason tietoaineiston vastaanottaja voi olla henkilö tai organisaatio. Suojaustasoon IV kuuluvaa tietoaineistoa saa lähettää sisäasiainministeriön hallinnonalan yhteisessä tietoliikenneverkossa salaamattomassa muodossa sähköisesti. Hallinnonalan ulkopuolelle IV suojaustason tietoaineistot tulee lähettää sähköisesti vahvasti salattuna. IV suojaustason aineistoa saa lähettää telekopiosanomana vastaanottaja varmistaen.

IV suojaustason tietoaineisto voidaan lisäksi lähettää vastaanottajalle manuaalilähetyksenä. Sähköisessä muodossa tallennetut manuaalilähetykset on vahvasti salattava. IV suojaustasoon kuuluva tietoaineisto lähetetään normaalin postin mukana suljetussa läpinäkymättömässä kirjekuoressa.

3.7 Tietoaineistojen hävittäminen

Tarpeettomaksi tullut tietoaineisto hävitetään arkistonmuodostussuunnitelman mukaisesti (säilyttäminen pysyvästi, lähettäminen Kansallisarkistoon tai määräajan säilytettävien hävittäminen).

I ja II suojaustasoihin luokiteltujen asiakirjojen jakelusta ja hävittämisestä on tehtävä asianmukaiset merkinnät diaariin.

Hävitettävä sähköisessä tai paperisessa muodossa oleva tietoaineisto poistetaan käytöstä joko tuhoamalla fyysisesti tai saattamalla sellaiseen muotoon, ettei niiden sisältämää tietoa voida käyttää.

I ja II suojaustasoihin luokitellut paperiset tietoaineistot hävitetään silppuamalla ne suojaustasovaatimuksen mukaisilla silppureilla tehtävään määrätyn henkilön toimesta. III ja IV suo-

jaustasoihin luokitellut paperiset tietoaineistot tuhotaan silppuamalla tai keräämällä ne lukittaviin paperinkeräysastioihin.

Hävitettävät, salassa pidettävää tietoa sisältäneet tai sisältävät muistivälineet kuten CD- ja DVD -levyt, magneettinauhat, kasetit, muistitikut, sekä -kortit toimitetaan lukittaviin säilytysastioihin. Muistivälineiden fyysinen tuhoaminen tapahtuu poliisihallinnon voimassaolevien sopimusten mukaisesti luotettujen kumppaneiden toteuttamana.

Käytöstä poistettavat tai huollettavat tietokoneet, älypuhelimet ja muut mahdollisesti kierrätettävät, tietoa sisältävät tai sisältäneet laitteet tai niiden massamuistit toimitetaan yksikön mahdollisen sisäisen ohjeistuksen mukaisesti yksikössä laitteita koordinoivalle taholle. Laitteiden massamuistien turvallinen tyhjennys toteutetaan poliisin tai Haltikin henkilöstön toimesta ennen luovuttamista ulkopuoliselle taholle.

Mikäli tietokoneilla, älypuhelimilla tai muilla kierrätettävillä laitteilla on käsitelty tai tallennettu salassa pidettävää tietoa, tulee turvallinen tyhjennys tehdä myös ennen siirtoa toiselle käyttäjälle. Vaatimus ei koske yhteiskäyttöön määritettyjä laitteita. Salassa pidettävää tietoa sisältäneitä siirrettäviä muistivälineitä kuten CD-levyjä, muistitikkuja ja vastaavia ei lähtökohtaisesti luovuteta eteenpäin.

Poliisin yksiköt järjestävät riittävän määrän silppureita ja keräysastioita henkilöstön käyttöön. Silppurit ja keräysastiat on merkittävä niillä tuhottavan tai niihin sijoitettavan tietoaineiston suojaustason mukaisesti. Astiat ja häkit on sijoitettava suojausluokan edellyttämään tilaan.

Eri suojaustasoille hyväksyttävät silppukoot:

SUOJAUSTASO IV (DIN 32757/4)

- palasen koko 2.0 mm x 15 mm ja palasen pinta-ala < 30 mm2

SUOJAUSTASOT III ja II (DIN 32757/4)

- palasen koko 2.0 mm x 15 mm ja palasen pinta-ala < 30 mm2

SUOJAUSTASO I (DIN 32757/5)

- palasen koko 0,78 mm x 11 mm ja palasen pinta-ala < 10 mm2

3.8 Tiedon antaminen salassa pidettävästä tietoaineistosta

Suojaustasomerkintä ei sellaisenaan vielä luo salassapitovelvollisuutta, vaan viranomaisen on arvioitava asiakirjan julkisuus joka kerta erikseen julkisuuslaissa edellytetyllä tavalla silloin, kun tietoaineistosta pyydetään tietoa.

Tietojen antamisesta salassa pidettävästä tietoaineistosta noudatetaan julkisuuslakia sekä erityislainsäädäntöä.

Mikäli poliisin yksiköltä pyydetään tietoa salassa pidettävästä tietoaineistosta, joka on toisen viranomaisen laatima, on asia siirrettävä ratkaistavaksi julkisuuslain mukaan tietoaineiston laatineelle viranomaiselle.

4 Poikkeukset

Tästä määräyksestä mahdollisesti poikkeavia käytäntöjä tai ratkaisuja koordinoivat yksiköiden tietoturvavastaavat ja -päälliköt. Päätös poikkeavan käytännön hyväksymisestä tehdään riski-analyysiin perustuen ja sen hyväksymisen tekee poliisin tietoturvapäällikkö kirjatun, perustellun poikkeama-pyynnön perusteella. Ratkaisut ovat määräaikaisia.

5 Ylläpito

Tämän määräyksen ylläpidosta ja ajantasaisuudesta vastaa poliisin tietoturvapäällikkö.

Liite 2: Tietoturvatasot poliisihallinnossa –määräys

TIETOTURVATASOT POLIISIHALLINNOSSA

Poliisin tietoturvallisuuteen liittyviä riskejä hallitaan yhdenmukaisella tavalla kaikissa poliisin yksiköissä. Poliisihallitus asettaa toiminnalle yleiset tavoitteet ja menettelytavat joita yksiköt noudattavat.

Tietoturvallisuuteen liittyvien riskien hallinnan tavoitteena on poliisin tietoturvapolitiikan (2020/2010/4157) tavoitteiden toteutuminen sekä lainsäädännön ja sopimusten vaatimusten täyttäminen.

Poliisin tietoturvallisuuden jatkuva arviointi ja toiminnan kehittäminen perustuu Valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010) määrittämien tietoturvatasojen vaatimuksiin.

Poliisin yksiköiden tulee täyttää tietoturvatasojen perustaso 1.1.2013 mennessä. 1.1.2015 mennessä kaikkien poliisin yksiköiden tulee täyttää vähintään tietoturvatasojen korotettu taso. Yksiköiden joissa käsitellään usein suojaustasojen II tai I tietoja, tulee täyttää tietoturvatasojen korkea taso 1.1.2015 mennessä vähintään niiden toimintojen osalta missä suojaustasojen I ja II tietoa käsitellään.

Poliisin yksikön johto tekee päätöksen tavoitellusta tietoturvatasosta niissä rajoissa mitä Poliisihallitus toiminnalle asettaa. Yksiköt voivat myös asettaa toiminnalleen tai kriittiseksi katsomilleen osille toiminnastaan korkeampia tavoitteita tai kehittää toimintaansa määritettyä nopeammassa aikataulussa.

1 Tietoturvatasovaatimukset

Poliisihallinnossa tietoturvatasojen vaatimuksilla käsitetään Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöön panosta (VAHTI 2/2010) liitteen 5 määrittämien tietoturvatasojen vaatimuksia sekä ohjeen ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin (VAHTI 2/2009) liitteen 3 vaatimuksia.

Poliisin tietoturvatasovaatimukset voidaan jakaa kolmeen erilliseen vaatimuslistaan

1. Vaatimukset organisaation tietoturvallisuuden hallinnalle
2. Tietojärjestelmien hallinnan kypsyyskriteerit
3. ICT-varautuminen

Kaikissa poliisin yksiköissä toteutetaan tietoturvatasojen vuosittainen läpikäynti sekä toiminnan arviointi tietoturvallisuuden hallinnollisen osuuden kriteerien osalta (kohta 1). Vaatimusten tulee täyttyä asetetun tietoturvatason mukaisesti annettuun määräaikaan mennessä.

Ne poliisin yksiköt joilla on omaa järjestelmäkehitystä tai tuottavat tai hallinnoivat tietotekniikkapalveluita, toteuttavat läpikäynnin vuosittain myös tietojärjestelmien hallinnan kypsyyskriteerien mukaisesti (kohta 2). Vaatimusten tulee täyttyä vaaditun tietoturvatason mukaisesti annettuun määräaikaan mennessä.

Ne poliisin yksiköt joilla on omaa järjestelmäkehitystä tai tuottavat tai hallinnoivat tietotekniikkapalveluita, toteuttavat läpikäynnin vuosittain myös ICT-varautumisen kypsyyskriteerien mukaisesti (kohta 3). Myös näihin vaatimuksiin liittyviä toimenpiteitä tulee kehittää riskien arviointiin perustuen, mutta vaatimusten täyttymistä ei vaadita tietoturvatason saavuttamiseksi.

2 Läpikäynnit ja kehittämistoimenpiteiden aikataulutus

Poliisin yksiköt käyvät tietoturvatasoihin liittyvät vaatimukset suhteessa omaan toimintaansa läpi vuosittain. Poliisin yksiköiden johto vastaa riittävästä resursoinnista jotta toiminta vastaa asetettuja tavoitteita.

Yksiköiden tietoturvatasoläpikäynneistä sekä tietoturvatasoihin liittyvästä kehittämisestä vastaa yksikön tietoturvapäällikkö tai -vastaava. Tietoturvapäällikkö tai -vastaava voi delegoida korjattavia tehtäviä sekä arviointi- ja läpikäyntityötä yksikössä.

Puutteet suhteessa annettuihin vaatimuksiin tunnistetaan ja niihin liittyvät riskit arvioidaan. Puutteiden korjaamiseksi suunnitellaan ja aikataulutetaan kehittävät toimenpiteet yksikön tietoturvallisuuden kehittämissuunnitelmaan. Toimenpiteille kirjataan vastuuhenkilö jonka vastuulla on korjauksen toteuttaminen. Kehittämissuunnitelman ja jäännösriskin hyväksyy yksikön johto niissä puitteissa missä Poliisihallitus toiminnan linjaa.

Tietoturvatasoarviointi toistetaan yksiköissä vuosittain ja kehittämissuunnitelmat päivitetään vastaamaan nykytilannetta vähintään vuosittain.

3 Poliisihallituksen toimenpiteitä vaativat kehittämistoimet

Poliisihallitus tukee yksiköiden tietoturvatason kehittämistyötä järjestämällä yksiköille koulutusta, tukea ja ohjausta sekä muodostaa linjauksia ja ohjeistusta niiden vaatimusten osalta

missä vaatimusten täyttämiseen vaadittava kehittämistyö on mahdollista ja käytännössä tehtävissä poliisihallinnon tasolla.

Poliisihallituksen tehtävä on myös tuottaa ja ylläpitää yhteisiä työkaluja poliisihallinnon tietoturvatasotyön tueksi.

4 Seuranta ja raportointi

Tietoturvatason kehittymisen seuranta ja ohjaus tapahtuu yksiköiden tietoturvapäälliköiden tai -vastaavien toimesta. Tietoturvapäälliköiden tai -vastaavien tehtävänä on kirjata läpikäyntien tulokset sekä suunnitellut ja tehdyt kehittämistoimenpiteet Poliisihallituksen ohjeistamaan tietoturvatasotyökaluun.

Yksikön tietoturvapäällikkö tai -vastaava raportoi tason kehittymisestä poliisin tietoturvaraportoinnin osana poliisin tietoturvapäällikölle sekä yksikön johdolle. Raportointi tarkoittaa yhteenvetoa poliisin yksikön tietoturvatasosta, edellisellä seurantajaksolla tehdyistä kehittämistoimenpiteistä sekä kehittämisaikataulun mukaisista suunnitelluista kehittämistoimenpiteistä seuraavalla seurantajaksolla.

Poliisin tietoturvapäällikkö seuraa yksiköiden tietoturvatason kehittymistä poliisihallinnon osalta ja raportoi poliisin ylimmälle johdolle tietoturvallisuuden kehittymisestä osana poliisin tietoturvaraportointia.

5 Tietoturva-auditoinnit

Poliisihallitus tai sen määrittämä taho tekee vuosittain tietoturvatasoihin liittyviä tarkastuksia. Tarkastukset ovat luonteeltaan ohjaavia mutta niiden päämääränä on myös todentaa yksiköiden tietoturvataso ja varmistaa Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) vaatimusten täyttyminen.

Tarkastukset toteutetaan siten että poliisin yksiköiden tietoturvataso tulee kokonaisuutena katselmoitua yksikön ulkopuolisen tahon toimesta vähintään neljän vuoden välein. Tarkastuksia voidaan toteuttaa yksikkökohtaisesti yksikön toiminta kokonaisuutena katselmoiden tai vaatimuskohtaisesti koko poliisihallinto katselmoiden.

6 Koulutus ja arvioijien pätevyysvaatimukset

Tietoturvatasoihin sekä tietoturvatasotarkastuksiin liittyvästä koulutuksesta ja valtakunnallisesta ohjeistuksesta vastaa Poliisihallitus.

Yksiköiden sisäisiä tietoturva-arviointeja ja -tarkastuksia saavat suorittaa poliisihallinnon sisäiseen tietoturvakoulutukseen osallistuneet sekä yksikön päätöksellä muilla tavoin riittävän pätevöityneet henkilöt. Yksittäisiä arviointi- ja kehittämistehtäviä tekeville henkilöille yksikön tietoturvapäällikön tai -vastaavan ohjauksessa ei vaadita erillistä koulutusta.

Yksiköissä suoritettavia ulkopuolisia tietoturvatasotarkastuksia tai muita arviointeja saavat suorittaa vain Poliisihallituksen määrittämät, tarkastuksiin koulutetut henkilöt.

7 Poikkeamat

Tästä määräyksestä mahdollisesti poikkeavia käytäntöjä tai ratkaisuja koordinoivat yksiköiden tietoturvavastaavat ja -päälliköt. Päätös poikkeavan käytännön hyväksymisestä tehdään riskianalyysiin perustuen ja sen hyväksymisen tekee poliisin tietoturvapäällikkö kirjatun, perustellun poikkeamapyynnön perusteella. Ratkaisut ovat määräaikaisia.

8 Ylläpito

Tämän määräyksen ylläpidosta ja ajantasaisuudesta vastaa poliisin tietoturvapäällikkö.

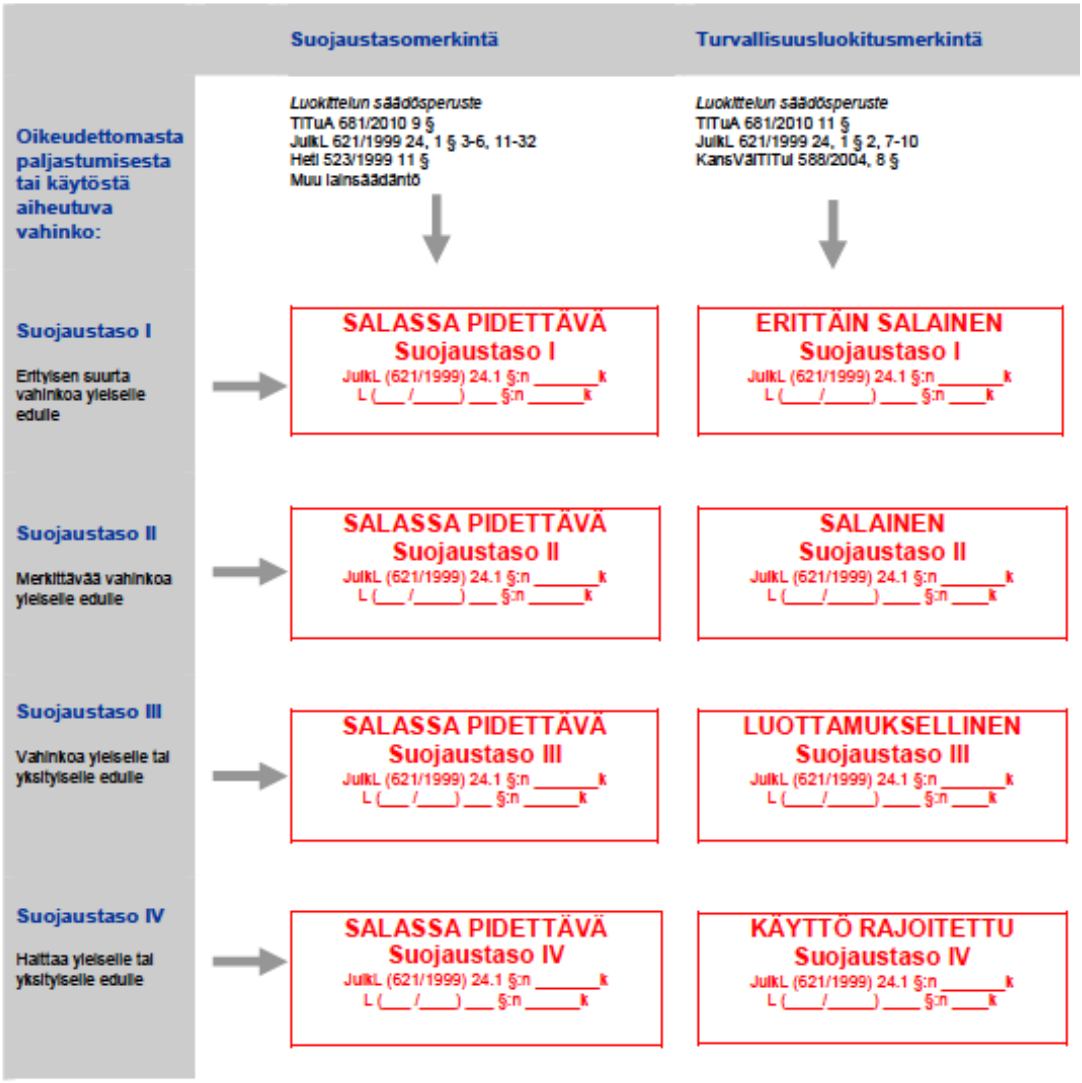
Liite 3: Huoneentaulu salassa pidettävien tietoaineistojen käsittelyyn

Salassa pidettävien tietoaineistojen käsittely

	SUOJAUSTASO IV	III	II	I
Käsittely, laatiminen				
Tietoverkosta erillään oleva poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Kyllä
Tietoverkkoon kytketty poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Ei
Poliisihallinnon mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Etäkäyttö	Kyllä	Kyllä	Ei	Ei
Tulostus ja kopiointi				
Verkkotulostin tai verkkoon kytketty monitoimilaite	Kyllä	Kyllä	Ei	Ei
Verkosta erillään oleva tulostin tai monitoimilaite	Kyllä	Kyllä	Kyllä	Kyllä
Kirjaaminen				
Julkinen diaari	Kyllä	Kyllä	Ei	Ei
Salaisten asiakirjojen diaari	Ei	Ei	Kyllä	Ei
Erittäin salaisten asiakirjojen diaari	Ei	Ei	Ei	Kyllä
Lähettäminen				
Kirjaamaton kirje	Kyllä	Ei	Ei	Ei
Kirjattu kirje, huomioitava ST II erityisvaatimukset	Kyllä	Kyllä	Kyllä	Ei
Kuriiripostina, huomioitava ST I ja II erityisvaatimukset	Kyllä	Kyllä	Kyllä	Kyllä
Salaamattomana sähköpostina poliisihallinnon ulkopuolelle	Ei	Ei	Ei	Ei
Salaamattomana sähköpostina poliisihallinnon sisällä	Kyllä	Ei	Ei	Ei
Salattuna sähköpostina	Kyllä	Kyllä	Kyllä	Ei
Fax, vastaanottaja varmistettava	Kyllä	Ei	Ei	Ei
Säilyttäminen, tallentaminen				
Murtosuojattu tila, kuten kassakaappi tai holvi	Kyllä	Kyllä	Kyllä	Kyllä
Lukittu kaappi tai muu vastaava tila	Kyllä	Kyllä	Ei	Ei
Tietoverkkoon kytketty poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Ei
Tietoverkosta erillään oleva poliisihallinnon työasema	Kyllä	Kyllä	Kyllä	Kyllä
Poliisihallinnon salatut tallennusmediat ja muistilaitteet	Kyllä	Kyllä	Kyllä	Kyllä
Poliisihallinnon mobiililaitteet	Kyllä	Kyllä	Ei	Ei
Hävittäminen				
Paperinkeräys	Ei	Ei	Ei	Ei
Lukittu tietosuojalaatikko ja ulkoisten medioiden lukitut keräyslaatikot	Kyllä	Kyllä	Ei	Ei
Silppuri, huomioitava silppurin luokitus (taso merkittävä silppuriin)	Kyllä	Kyllä	Kyllä	Kyllä

1.1 - 24.1.2011

Salassa pidettävien asiakirjojen luokittelu ja merkitseminen



Turvallisuusluokka	Nimike	Lyhenne	Nimike ruotsiksi
Turvallisuusluokka I	ERITTÄIN SALAINEN	ERSAL (E)	YTTERST HEMLIG
Turvallisuusluokka II	SALAINEN	SAL (S)	HEMLIG
Turvallisuusluokka III	LUOTTAMUKSELLINEN	LUOT (L)	KONFIDENTIELL
Turvallisuusluokka IV	KÄYTTÖ RAJOITETTU	RAJ (R)	BEGRÄNSAD TILLGÅNG

1.1 - 24.1.2011