VALTIOVARAINMINISTERIÖ

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta

Valtionhallinnon tietoturvallisuuden johtoryhmä

2/2010 VAHTI

VALTIOVARAINMINISTERIÖ

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta

Valtionhallinnon tietoturvallisuuden johtoryhmä

2/2010 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi

ISSN 1455-2566 (nid.)
ISBN 978-952-251-125-6 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-124-9 (PDF)

VALTIOVARAINMINISTERIÖ
Hallinnon kehittämisosasto

VM/2029/00.00.00/2010
OHJE
19.10.2010

Ministeriöille, virastoille ja laitoksille

OHJE TIETOTURVALLISUUDESTA VALTIONHALLINNOSSA ANNETUN ASETUKSEN TÄYTÄNTÖÖNPANOSTA

Valtiovarainministeriön *Ohjeen tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta* tavoitteena on tehostaa ja yhdenmukaistaa lain viranomaisen toiminnan julkisuudesta (621/1999) perusteella 1.7.2010 annetun ja 1.10.2010 voimaantulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanoa. Ohjeen mukaisella toiminnalla viranomainen voi saavuttaa toiminnassaan ja yhteistyössään asetuksen mukaisen tietoturvatason, joka tasapainottaa riskienhallinnan ja kustannustehokkuuden. Ohje korvaa aiemmat ohjeet Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VAHTI 2/2000), Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje (VM 5/01/2000) sekä Arkaluonteiset kansainväliset tietoaineistot (VAHTI 4/2002).

Ohje on tarkoitettu organisaatioiden johdolle ja henkilökunnalle sekä niiden toimintaprosesseista, turvallisuudesta, tietopalveluista ja tietohallinnosta vastaaville.

Viranomaisen on saatettava toimintansa ja tietojenkäsittelynsä vastaamaan asetuksessa säädettyjä perustason tietoturvavaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä. Ohjeeseen sisältyy tarkemmat perus-, korotetun ja korkean tietoturvatason linjaukset. Tietoturvatasojen toteuttamista koskeva selvitys- ja valmistelutyö on tarpeen organisoida viranomaisissa syksyn 2010 aikana.

Tietoaineistojen luokittelun käyttöönoton suunnittelu on tärkeää. Luokituksen on määrä helpottaa viranomaisten välistä salassa pidettävien tietojen vaihtoa. Viranomaisen on syytä päättää, ottaako se luokittelun käyttöön ja milloin. Luokittelua vastaavat käsittelyvaatimukset on toteutettava viiden vuoden kuluessa siitä, kun luokittelu otetaan käyttöön. Viranomaisella on mahdollisuus kohdistaa luokittelu vain tiettyihin asiakirjoihin tai sellaisiin asiakirjan käsittelyvaiheisiin, joissa toimenpiteet suojattavan edun vuoksi ovat tarpeen. Osa kansainvälisistä aineistoista on pakko luokitella säädösten mukaisesti.

Valtionhallinnon organisaatioiden tulee toiminnassaan ottaa huomioon ohjeessa kuvatut linjaukset. Organisaatioiden, toimintojen, palveluiden, järjestelmien, tietoaineistojen, toimitilojen ja riskienhallinnan sekä osaamisen, koulutuksen ja yhteistyön kehittämiseen ja hallintaan tulee valtionhallinnon organisaatioissa sisällyttää asetuksen ja ohjeen mukaisesti tietoturvaasiat ja niiden varmistaminen.

Hallinto- ja kuntaministeri — Tapani Tölli

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)

Virastojen johdolle

Tietoturvallisuuden tarkoituksena valtionhallinnossa on varmistaa viranomaisen toiminnan jatkuvuus ja laatu sekä oikeusturvan toteutuminen. Tässä ohjeessa annetaan ohjeet tietoturvallisuudesta valtionhallinnossa annetun asetuksen (681/2010; jäljempänä tietoturvallisuusasetus, TTA) täytäntöönpanosta.

Ohje on tarkoitettu organisaatioiden johdolle sekä niiden toimintaprosesseista, turvallisuudesta, tietopalveluista ja tietohallinnosta vastaaville

Valtionhallinnon viranomaisten yleinen velvollisuus huolehtia tietoturvallisuudesta perustuu viranomaisten toiminnan julkisuudesta annettuun lakiin (621/1999; jäljempänä julkisuuslaki, JulkL). Lain mukaan viranomaisten on huolehdittava, että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvajärjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvatoimenpiteistä aiheutuvat kustannukset (18 § 2 mom. 4 k).

Valtioneuvoston 1.7.2010 julkisuuslain nojalla antamaa tietoturvallisuusasetusta sovelletaan valtionhallinnon viranomaisiin. Näillä tarkoitetaan valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia (3 § 1 k). Asetuksella kumottiin viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallinta-tavasta annetun asetuksen (1030/1999; jäljempänä julkisuusasetus, JulkA) 2 ja 3 §.

Tietoturvallisuusasetus tuli voimaan 1.10.2010. Asetukseen sisältyy siirtymäaikaa koskevat säännökset. Näiden mukaan viranomaisen on saatettava tietojenkäsittelynsä vastamaan asetuksen 5 §:ssä säädettyjä perustason tietoturvavaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä.

Asetuksessa säädetään viranomaisen asiakirjojen käsittelyä koskevista yleisistä tietoturva-vaatimuksista sekä asiakirjojen luokittelusta ja niitä vastaavista asiakirjojen käsittelyä koskevista vaatimuksista. On syytä huomata, että asiakirjalla tarkoitetaan asetuksessa myös sähköisessä muodossa tai muutoin teknisenä tallenteena talletettuja tietoaineistoja. Sääntely kohdistuu ensijäisesti salassa pidettäviin asiakirjoihin (TTA 8 §; 9 § 2 mom.).

Asiakirjojen luokittelu ei asetuksen mukaan ole pakollista. Viranomaisen on syytä päättää, ottaako se luokittelun käyttöön ja milloin. Luokittelua vastaavat käsittelyvaatimukset on toteutettava 5 vuoden kuluessa siitä, kun luo-

kittelu otetaan käyttöön. Viranomaisella on mahdollisuus kohdistaa luokittelu vain tiettyihin asiakirjoihin tai sellaisiin asiakirjan käsit-telyvaiheisiin, joissa toimenpiteet suojattavan edun vuoksi ovat tarpeen (TTA 8 § 1 mom.)

Luokittelun käyttöönoton suunnittelu on tärkeää. Luokituksen on määrä helpottaa viranomaisten välistä salassa pidettävien tietojen vaihtoa, minkä vuoksi luokittelu on erityisen suositeltavaa toteuttaa viranomaisissa, jotka joko saavat toisilta viranomaisilta tai luovuttavat muille viranomaisille säännönmukaisesti ja massaluonteisesti salassa pidettäviä asiakirjoja.

Virastoissa on tarpeen varmistaa, että kaikki tietoturvallisuusasetuksen 5 §:ssä säädetyt tietoturvallisuuden perustason vaatimukset täytetään asetuksessa edellytetyssä kolmen vuoden siirtymäajassa. Tätä koskeva selvitys- ja valmistelutyö on tarpeen organisoida syksyn 2010 aikana.

Tietoturvavaatimusten ja yleisemminkin julkisuuslaissa säädetyn hyvän tiedonhallintatavan toteuttamiseksi on viranomaisen tärkeätä varmistaa, että

- viranomaisen hallussa olevat asiakirjat on kartoitettu ja niihin sisältyvien tietojen merkitys arvioitu julkisuusasetuksen 1 §:ssä säädetyllä tavalla. Toimintaan liittyvät tietoturvariskit on kartoitettu ja tietoturvallisuuden toteuttaminen on suunniteltua (TTA 4 §, 5 § 1 mom.1 k),
- viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
- asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään ja 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;
- tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
- 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;
- asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
- henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
- henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;

- annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti;
- toteutetaan järjestelyt, joiden avulla voidaan varmistaa, että asetettuja tietoturvavaatimuksia noudatetaan myös silloin, kun viranomaisen asiakirjoja käsitellään toimeksiantosopimuksen perusteella esim. tietojenkäsittelyn palveluyrityksissä (TTA 6 §);
- pidetään huolta, että virkamiehet tietävät luokittelumerkintöjen merkityksen ja sen, että ne eivät vapauta viranomaista velvollisuudesta asiakirja- ja tapauskohtaisesti arvioida julkisuuslain ja sen ratkaisukäytännön mukaisesti asiakirjan julkisuutta siitä tietoja julkisuuslain nojalla pyydettäessä.

Tietoturvallisuusasetus ja tämä ohje ovat tärkeä osa valtiohallinnon tietoturvallisuuden kehittämistä koskevan valtioneuvoston periaatepäätöksen 26.11.2009 toimeenpanoa.

Tämä ohje korvaa VAHTIn aikaisemmat ohjeet Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VAHTI 2/2000) ja Arkaluonteiset kansainväliset tietoaineistot (VAHTI 4/2002). Ohje on näitä edellisiä huomattavasti kattavampi.

Lyhyesti VAHTIsta

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuden linjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTI edistää hallitusohjelman, Yhteiskunnan elintärkeiden toimintojen strategian (YETT), valtion IT-strategian, valtioneuvoston huoltovarmuuspäätöksen, kansallisen tietoturvastrategian, valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä.

Valtioneuvosto teki 26.11.2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätös korostaa VAHTIn asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elimenä. Peiaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTIssa koordinoitavaan yhteistyöhön.

VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta astaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu yksi maailman kattavimmista yleisistä tietoturvaohjeistoista (www.vm.fi/vahti). VM:n ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita sekä laaja valtion tietoturvallisuuden kehitysohjelma.

VAHTI on saanut kolme kertaa tunnustuspalkinnon esimerkillisestä toiminnastaan Suomen tietoturvallisuuden parantamisessa.

Sisältö

1 Johdanto

1.1 Tarkoitus ja soveltamisala

Tämän ohjeen tarkoituksena on edistää hyvän tiedonhallintatavan toteuttamista valtionhallinnossa sekä valtionhallinnon tietoturvallisuudesta annetun asetuksen (TTA, tietoturvallisuusasetus, 681/2010) täytäntöönpanoa.

Ohjeessa kuvataan vaatimuksia hyvän tiedonhallintatavan mukaisten toimintaedellytysten toteuttamiseksi organisaatiossa. Näitä ovat mm. velvoite tietovarannon suunnittelusta sekä vaatimukset tietoverkoille, tietojärjestelmille, toimitiloille, asiakirjahallinnolle ja käyttövaltuushallinnolle. Toimenpiteiden tarkoituksena on luoda tietotyötä suorittaville turvallinen ja tehokas työympäristö tiedon käsittelylle kaikissa elinkaaren vaiheissa.

Tietoturvallisuusasetuksen ja näiden ohjeiden tavoitteena on luoda edellytykset valtionhallinnon tietoturvatyön kehittämiseksi sekä yhtenäisten menettelyjen luomiseksi salassa pidettäviä ja käytöltään rajoitettuja tietoaineistoja käsiteltäessä. Asetusta laadittaessa on otettu huomioon valtiovarainministeriössä laadittu suunnitelma erilaisten tietoturvallisuustasojen toteuttamisesta valtionhallinnossa. Sen avulla vahvistetaan valtiovarainministeriön hallinnon kehittämisosaston informaatio-ohjaukseen perustuvaa kehittämistyötä ja tämän ohjauksen merkitystä.

Uudistuksen on määrä myös vahvistaa hallinnon asiakkaiden ja sidosryhmien luottamusta hallintoon ja sen tietojenkäsittelyyn sekä luoda asianmukaiset puitteet sähköisen asianhallinnan ja sähköisten palvelujen kehittämiselle. Yhtenäisillä menettelyillä luodaan edellytykset tietoaineistojen turvalliseen käsittelyyn viranomaisten ja näiden lukuun toimivien tietopalvelutoimittajien ja viranomaistietoa käsittelevien osapuolten kanssa.

Ohje käsittelee erityisesti salassa pidettävän tiedon suojaamista. Tietoaineistoja käsitellään neljälle eri suojaustasolle (katso luku 5) asetettujen teknisten ja toiminnallisten vaatimusten mukaisesti. Ohjeessa otetaan huomioon myös muu Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) antama ohjeisto, jossa on asetettu tarkempia vaatimuksia erilaisiin käsittelyvaiheisiin ja teknisiin tai hallinnollisiin toimintoihin.

Asiakirjoilla tarkoitetaan julkisuuslain 5 §:ssä määriteltyjä asiakirjoja, jotka ovat myös sähköisessä muodossa tai muutoin teknisenä tallenteena talletettuja

tietoaineistoja. Tietoaineistoilla tarkoitetaan tässä ohjeessa paperilla, sähköisillä tai muilla tietovälineillä olevia asiakirjoja ja tietoja.

Ohjeessa määritellään vaatimuksia hyvän tiedonhallintatavan mahdollistavien toimintojen toteuttamiseksi, jotta tietoaineistojen käyttäjät voivat kaikissa käsittelyvaiheissa toimia asetettujen vaatimusten mukaisesti.

Ohjeeseen sisältyy ohjeet asiakirjojen ja tietojen luokituksesta ja suojaamisesta sekä käsittelyn elinkaaren eri vaiheiden turvallisuusvaatimuksista ja suositeltavista käytännöistä. Ohjeessa on otettu huomioon myös henkilötietolain (523/1999, jäljempänä HetiL, henkilötietolaki) asettamat erityisvaatimukset henkilötietojen käsittelyn osalta. Ohje sisältää myös vaatimukset viranomaisen asiakirjojen käsittelemisestä ulkopuolisten palveluntuottajien osalta.

Ohjeessa kuvataan hyvän tiedonhallintatavan ja tietoturvallisuuden varmistamistarpeiden mukaiset tietojen luokituskäytännöt erityisesti tietojen salassapidon ja niiden käyttörajoitusten huomioon ottamiseksi sekä tähän luokitteluun perustuvien tietojen käsittelyohjeet. Lisäksi on määritelty yleisesti eheyteen ja käytettävyyteen liittyviä vaatimuksia.

Ohjeessa käsitellään tietojen ja asiakirjojen tietoturvavaatimuksia sekä manuaalisen että sähköisen käsittelyprosessin eri vaiheissa. Tietoturvavaatimukset on määritelty luvussa 4. Ohjeessa on otettu huomioon erityisesti asianhallinta-tyyppinen asiantuntijatyö, jossa käsitellään sekä paperimuotoisia että sähköisiä asiakirjoja. Ohjetta suositellaan käytettäväksi soveltuvin osin myös vakiomuotoisessa tietojärjestelmien ja tietokantojen hyväksikäyttöön perustuvassa tiedonkäsittelyssä.

Tämä ohje on sisällöltään yleisluontoinen. Liiteosuuksiin on koottu yksityiskohtaisempaa tietoa perusteista, salassa pidettävän tiedon merkitsemisestä ja käsittelystä sekä erityiset muistilistat eri kohderyhmille heitä koskevista velvoitteista. Liitteessä 4 asetettujen yksityiskohtaisten velvoitteiden toivotaan ohjaavan kunkin hallinnonalan toimintaa. Tässä korostetaan hyvän tiedonhallintatavan toteuttamisen edellytysten mahdollistumista myös niiltä osin, joissa viranomaisen tietoja käsitellään eri tahoilla.

Ministeriöt huolehtivat hallinnonalansa henkilöstön koulutuksesta ja antavat tarvittaessa hallinnonalaansa koskevia soveltamisohjeita tämän ohjeen pohjalta.

Tietojenkäsittely-ympäristöt luokitellaan perus-, korotetun ja korkean tietoturvallisuustason ympäristöiksi. Samaa luokitteluasteikkoa käytetään myös tietoturvallisuuden hallintajärjestelmän tason määrittelyssä.

Kansainväliseen yhteistyöhön liittyviä (esim. EU, NATO, OECD) asiakirjoja käsittelevien organisaatioiden tulee ottaa huomioon kansainväliset tietoturvallisuusvelvoitteet (ks. L kansainvälisistä tietoturvallisuusvelvoitteista; 588/2004). Näiden vaatimusten osalta yksityiskohtaista tietoa antaa tarvittaessa ulkoministeriön NSA-yksikkö.

Kukin organisaatio tarkentaa vaatimuksia omassa ohjeistuksessaan toiminnan tarpeiden ja tietoturvavaatimusten perusteella. Yksityiskohtaisemmat

ohjeet ja kuvaukset näkyvät mm. tietojärjestelmien kuvauksissa, käyttöohjeissa ja arkistonmuodostussuunnitelmassa sekä henkilötietojen osalta rekisteri- tai tietosuojaselosteissa. Ministeriön, viraston ja laitoksen tulee huolehtia henkilöstön perehdyttämisestä tietoaineiston käsittelyn ohjeistukseen.

Asiakirjojen sisällön, luokittelun ja käsittelyn virastokohtainen arviointi tulee tehdä tietoturvallisuuden varmistamiseksi osana toiminnan sekä sen laadun ja jatkuvuuden varmistamista.

1.2 Ohjeen rakenne

Ohje koostuu kuudesta pääluvusta ja kuudesta liitteestä.

Ensimmäisessä pääluvussa kerrotaan ohjeen tarkoitus ja tavoitteet. Toinen pääluku kuvaa ohjeen toimeenpanoon liittyvät osuudet. Kolmannessa pääluvussa esitetään hyvän tiedonhallinta- ja hyvän tietojenkäsittelytavan toteuttamisen edellytyksiä tietoaineistojen käsittelemiseksi. Tämä osuus on rakenteeltaan luettelonomainen. Neljännessä pääluvussa esitetään vaatimukset viranomaiselle toimenpiteistä, joilla mahdollistetaan turvallinen asiakirjojen käsittely. Viidennessä pääluvussa esitetään tietoaineistojen luokitukseen ja merkintään liittyvät vaatimukset ja velvoitteet. Kuudennessa pääluvussa esitetään käsittelyvaatimukset tietoaineistojen eri käsittelyvaiheille. Asiat käsitellään yleisellä tasolla ottaen huomioon kaikki elinkaaren vaiheet.

Liitteissä tarkennetaan tekstiosuuden sisältöä. Säädösluettelo esitetään liitteessä 1. Liitteessä 2 esitetään salassa pidettävän tietoaineiston käsittelyssä tarvittavat leimat ja merkinnät. Liitteessä 3 annetaan viranomaiselle ohjeet vaadittavista toimenpiteistä turvallisen tietotyön mahdollistamiseksi. Asiakirjojen suojaustasokohtaiset käsittelyohjeet on esitetty liitteessä 4, tietoturvallisuustasojen vaatimukset liitteessä 5 sekä korvaava menettely liitteessä 6.

Ohje on tarkoitettu käytettäväksi laajasti hallinnon eri toiminnoissa, prosesseissa, palveluissa, järjestelmissä, asiakirjoissa ja hankinnoissa. Tämän ohjeen eri luvut antavat myös tiedon käyttäjälle hyvää lisätietoa.

1.3 Tietoturvallisuustasot

Tietoturvallisuustasojen avulla määritellään organisaatiolle ja tietojenkäsittely-ympäristöille tekniset ja hallinnolliset vaatimukset.

Tietoturvallisuustasot kuvaavat niitä tietoturvatoimintaan ja -prosesseihin liittyviä vaatimuksia, jotka jokaisessa valtionhallinnon organisaatiossa tulee toteuttaa. Vaatimusten toteuttamisvelvoitetta ei ole aiemmin sisällytetty lainsäädäntöön, mutta niiden täyttämistä on voitu edellyttää muulla tavoin. Osa vaatimuksista sisältyy jo julkishallinnolle asetettuihin velvoitteisiin hyvän tiedonhallintatavan noudattamisesta. Myös Valtion IT-palvelukeskus voi palve-

luita tarjotessaan edellyttää, että sen asiakkaat täyttävät tietoturvallisuustasoissa asetetut vaatimukset.

Tietojenkäsittely-ympäristöt ja hallinto luokitellaan kolmeen tasoon: tietoturvallisuuden perustaso, korotettu taso ja korkea taso. Alin viranomaisen tietojenkäsittely-ympäristöille sallittu taso on tietoturvallisuuden perustaso. Tässä ympäristössä voidaan tietosisällön toimivaltaa käyttävän viranomaisen päätöksellä käsitellä selväkielisessä muodossa suojaustason IV edellyttävää tietoa (katso luku 7.4). Korotetun tietoturvallisuustason ympäristössä voidaan vastaavilla valtuuksilla käsitellä tietoa selväkielisessä muodossa aina suojaustasoon III asti. Vastaavasti korkean tietoturvallisuustason täyttävissä ympäristöissä voidaan käsitellä tietoa selväkielisessä muodossa suojaustasoon II asti.

Tietoturvallisuustasojen vaatimukset on ryhmitelty kahteen osakokonaisuuteen: (1) hallinnollisen tietoturvallisuuden ja (2) teknillisen tietoturvallisuuden vaatimukset. Tietoturvallisuustasoja on käsitelty tarkemmin luvuissa 5 ja 6 sekä liitteessä 5.

Viranomainen voi varmistaa järjestelmiensä tietoturvallisuustason käyttämällä erilaisia arviointitapoja. Tällaisia ovat viranomaisen itsearvioinnit sekä tietoturva-auditointia tarjoavien yritysten ja viranomaistahojen palvelujen käyttö. Näillä menetelmillä viranomaisen tietoturvallisuustoimien taso arvioidaan suhteessa tietoturvallisuusasetukseen ja näihin ohjeisiin taikka, jos kysymys on esim. EU-asiakirjojen käsittelystä, suhteessa EU:n turvallisuussääntöihin.

Hallinnon sisäverkoille annetuista tietoturvatasovaatimuksista on oma VAHTI-ohje (3/2010).

1.4 Tietoaineistojen käsittely ja hallinta

Tiedon merkitys yhteiskunnassa ja viranomaisen toiminnassa korostuu kaiken aikaa. Viranomaisen toiminnalliset tavoitteet asettavat tiedon hallinnalle suuria haasteita.

Hyvän tiedonhallintatavan toteuttaminen edellyttää tiedon elinkaaren hallintaa. Elinkaaren toteuttamista ohjataan arkistolaissa (831/1994, jäljempänä ArkL) määritellyn arkistonmuodostussuunnitelman avulla.

Henkilötietojen käsittelyssä on otettava huomioon henkilötietolaki ja sen säännökset mm. huolellisuusvelvollisuudesta ja hyvästä tietojenkäsittelytavasta.

Viranomaisen on arvioitava käytössään olevan tietovarannon ja tietovarantoa käyttävien tietojärjestelmien sekä käsittelyprosessien ajantasaisuus.

Tietoaineiston käsittelyn arvioinnissa tulee kiinnittää huomiota Tietoturvallisuuden arviointi valtionhallinnossa -ohjeessa (VAHTI 8/2006) esitettyjen kysymysten vaatimuksien toteutumiseen.

1.5 Lainsäädäntö ja kansainväliset velvoitteet

Salassa pidettävien asiakirjojen käsittelyssä on noudatettava erityistä huolellisuutta. Tätä koskevat velvoitteet sisältyvät julkisuuslakiin. Virkamiehen ja julkisyhteisön työntekijän salassapitovelvollisuuden rikkomisesta säädetään rikoslain 40 luvussa ja muiden henkilöiden salassapitorikoksesta ja rikkomuksesta rikoslain 38 luvussa.

Julkisuuslain mukaan viranomaisen asiakirjat ovat julkisia, jollei lailla toisin säädetä. Asiakirjan käsite on julkisuuslaissa laaja ja se kattaa myös erilaiset tekniset tallenteet (5 §). Yleisimmät salassapitoperusteet ovat julkisuuslain 24 §:ssä. Erityissäännöksiä sisältyy lisäksi jonkin verran myös muuhun lainsäädäntöön. Julkisuuslain mukaan jokaisen asiakirjan julkisuus on selvitettävä tapauskohtaisesti silloin, kun joku pyytää asiakirjaa nähtäväkseen tai saadakseen siitä kopion. Julkisuuslain 17 §:ssä säädetään tulkintaohjeet: salassapitoa ei saa ulottaa laajemmalle kuin suojattava etu vaatii. Jos asiakirjasta vain osa on salassa pidettävää, viranomaisen on annettava asiakirjasta tieto muilta osin (10 §). Viranomaisen on tehtävä päätös kieltäytyessään antamasta tietoa asiakirjasta. Viranomaisen on perusteltava huolellisesti päätös tiedonsaannin epäämiselle. Lisätietoa julkisuuslain soveltamisesta löytyy oikeusministeriön kotisivuilta www.om.fi. (Perussäännöksiä, Julkisuuslaki, Oikeusministeriön 23.9.2005 ministeriöille julkisuuslainsäädännön täytäntöönpanosta ja osittaistarkistuksesta lähettämä kirje liitteineen).

Julkisuuslain hyvää tiedonhallintatapaa koskevat säännökset (18 §) edellyttävät muun ohella, että viranomainen antaa henkilöstölle ohjeet julkisuuslain toteuttamisesta.

Salassa pidettävästä asiakirjasta saa lain mukaan antaa tiedon vain viranomainen tai se virkamies, jolle tällainen oikeus on nimenomaisesti työjärjestyksessä tai vastaavalla tavalla annettu.

Asiakirjasta, joka ei julkisuuslain 6 ja 7 §:n mukaan ole vielä tullut julkisuusarvioinnin piiriin (harkinnanvaraisesti julkiset asiakirjat), saa tiedon antaa viranomainen tai viranomaisen antaman yleisen ohjauksen mukaisesti esim. asiaa valmisteleva virkamies. Huomaa, että viranomaisella on julkisuuslain 19 §:n mukaan velvollisuus antaa tietyistä valmisteilla olevista asioista suullisesti tietoa.

Tietoturvallisuuden varmistamiseksi tehtävä asiakirjojen luokittelu ja sitä vastaavien merkintöjen tekeminen asiakirjaan ei muuta edellä kuvattua velvollisuutta arvioida asiakirjan julkisuus erikseen ja tapauskohtaisesti silloin, kun viranomaiselta pyydetään asiakirjaa. Ainoa poikkeus tästä säännöstä ovat asiakirjat, joihin on tehty turvallisuusluokitusmerkintä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) 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.

Aineiston käsittelyä koskevia keskeisiä säädöksiä ja ohjeita:

Lakeja ja kansainvälisiä linjauksia:	Valtionhallinnon tietoturvallisuuden ohjeistusta:
Arkistolaki (831/1994) 7§, 8§, 4. luku	Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004 luku 4.2)
Henkilötietolaki (523/1999)	Keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004, luku 5)
Julkisuuslaki (JulkL, 621/1999) 1§, 3 §, 10 §, 5. luku, 6. luku, 7. luku Julkisuusasetus (JulkA, 1030/1999) 1 § Tietoturvallisuusasetus (TTA, 681/2010).	Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003 luku 2)
Laki kansainvälisistä tietoturvallisuus velvoitteista (588/2004)	Tietoturvallisuuden arviointi valtionhallinnossa (VAHTI 8/2006 Liite 3)
Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, VM 0024:00/02/99/1998	Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005, luku 2.1.1)
Valmiuslaki (1080/1991)	Kansainvälinen tietoturvatyö (VAHTI 1/2007)
Sähköisen viestinnän tietosuojalaki (516/2004), 2. luku, 3. luku, 5. luku	Lokien käsittelyohje (VAHTI 3/2009)
Laki turvallisuusselvityksistä (177/2002)	Henkilöstöturvallisuusohje (VAHTI 2/2008)
Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta, sivut 24, 33, VM 2005	Tietotekniikan turvallisuus ja toiminnan varmistaminen (PTS 1/2002, luku 3.2)

Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä.

– Laki viranomaisen toiminnan julkisuudesta, 18 §

Tietoturvallisuuden johtaminen on kiinteä osa organisaation toiminnan johtamista. Sen tulee siten sisältyä jokaisen johtotehtävissä toimivan henkilön vastuisiin. Tietoturvallisuus toteutuu parhaiten olleessaan sisäänrakennettuna organisaation suunnitteluprosesseissa (toiminnan kehittäminen), laatu- ja muissa seurantajärjestelmissä (arviointi, mittaaminen) sekä tavoitteiden saavuttamisen seurannassa.

– Tietotekniikan turvallisuus ja toiminnan varmistaminen, PTS 2002

Johdon tulee olla tietoinen organisaation tietoturvallisuuden tasosta ja tietoturvariskien hallinnan tilasta. Tällöin tulee olla selvillä, mikä on tietoturvallisuuden lähtökohtainen tila, tietoturvatoiminnan merkitys toiminnalle ja kullekin toiminnolle suhteessa sen kriittisyyteen. Tietoturvallisuuden kehittäminen edellyttää asetettuun tavoitetilaan tähtäävää kehittämisohjelmaa ja sen seurantaa.

– Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003, luku 2

1.6 Ohjeen keskeisimmät käsitteet

Asiakirja: Asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla (Julkisuuslaki 5 § 1 mom.; ks. myös tietoturvallisuusasetus 3 § 3 k). Asiakirjan käsite on siten riippumaton siitä, minkälaiselle alustalle tai minkälaisin keinoin tieto on talletettu. Siten asiakirjoilla tarkoitetaan paitsi perinteisiä paperimuotoisia asiakirjoja, myös sähköisesti talletettuja tietoaineistoja riippumatta niiden muodosta.

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

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

Henkilörekisteri: Henkilörekisterillä tarkoitetaan henkilötietolain 3 §:n 3 kohdan mukaan ’käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa tietojoukkoa, joka 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). Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.

Henkilötietojen käsittely: Henkilötietojen käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä (henkilötietolaki 3 § 2 k).

Luokiteltu asiakirja: Luokitellulla asiakirjalla tarkoitetaan tässä ohjeessa asiakirjaa, joka on luokiteltu tietoturvallisuusasetuksen mukaan kuuluviksi johonkin suojaustasoon asetuksen 9 §:n mukaisesti ja siinä säädetyin edellytyksin. Kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvan asiakirjan luokittelusta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa.

Rekisterinpitäjä: Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä ja säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on säädetty (henkilötietolaki 3 § 4 k).

Rekisteriseloste: Rekisteriseloste on henkilötietolain edellyttämällä tavalla (henkilötietolaki 10 §) laadittu ja saatavilla pidettävä määrämuotoinen kuvaus henkilörekisterin sisällöstä, käytöstä ja suojauksesta.

Salassa pidettävä asiakirja: Salassa pidettävällä asiakirjalla tarkoitetaan niitä asiakirjoja ja tietoja, jotka ovat julkisuuslain 24.1 § mukaan salassa pidettäviä.

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 (luku 7.3, Tietoturvallisuusasetus, 9 §).

Tietosuojaseloste: Henkilötietoja käsittelevän tahon selvitys siitä, miten se käsittelee henkilötietoja ja miten henkilötietolain mukaiset rekisteröidyn oikeudet toteutetaan.

Tietoturvallisuustasot: Tietoturvallisuustasoilla tarkoitetaan niitä teknisiä ja hallinnollisia järjestelyjä, joiden avulla varmistetaan eritasoisten tietoturvallisuuden toteuttaminen. **Perustason** vaatimukset täyttävässä ympäristössä voidaan toteuttaa suurin osa viranomaisen tiedonkäsittelytarpeista. Niiden asiakirjojen käsittelyssä, jossa edellytetään korkeaa luotettavuutta kaikissa toimintaolosuhteissa ja jossa käsitellään laajasti suojaustasoa III edellyttävää luokiteltua tietoa, viranomaisen on ylläpidettävä **korotetun tietoturvallisuustason** täyttäviä rakenteita. Kriittiset ja laajasti suojaustasoon II luokiteltua tietoa sisältävät tietojärjestelmät tulee toteuttaa **korkean tietoturvallisuustason** ympäristöissä. Suojaustasoa I edellyttäviä asiakirjoja voidaan käsitellä korkean tietoturvallisuustason vaatimukset täyttävissä **erillisverkoissa**, joissa ei ole yhteyttä muihin verkkoihin.

Toimivaltainen viranomainen: Toimivaltaisella viranomaisella tarkoitetaan sitä viranomaista, jolle säädettyjen tehtävien hoitamista (käyttöä) varten asiakirja laaditaan tai toimitetaan ja jolla on oikeus päättää asiakirjan luovuttamisesta ja määrätä sen muusta käsittelystä. Toimivaltaisella viranomaisella on vastuu toimintaansa liittyvistä tietojärjestelmistä ja asiakirjoista. Tietohallinto- ja tietoturvatyössä käytetään usein toimivaltaisesta viranomaisesta tai muusta organisaatiosta 'tietojärjestelmien omistaja-käsitettä'.

Toimivaltainen virkamies: Asianomaisessa viranomaisessa asiakirjan käsittelystä ja luokittelusta vastaava virkamies, jolle tehtävä työjärjestyksen tai muun

vastaavan määräyksen perusteella kuuluu ja jolla sen perusteella on oikeus määrätä asiasta.

Turvallisuusluokiteltava asiakirja: salassa pidettävää tietoaineistoa sisältävä asiakirja, johon voidaan tietoturvallisuusasetuksen tai kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan tehdä turvallisuusluokkaa osoittava merkintä ja jonka käsittelyssä on noudatettava luokkaa vastaavia tietoturvavaatimuksia. Turvallisuusluokiteltavien asiakirjojen nimikkeet suojaustasoittain ovat: **ERITTÄIN SALAINEN** (suojaustaso I), **SALAINEN** (suojaustaso II), **LUOTTAMUKSELLINEN** (suojaustaso III) ja **KÄYTTÖ RAJOITETTU** (suojaustaso IV).

Turvallisuusluokittelumerkintä: Turvallisuusluokittelumerkintä voidaan tehdä sellaiseen asiakirjaan, jonka tietojen oikeudeton paljastuminen voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille julkisuuslain 24 §:n 1 momentin 2, 7 – 10 kohdissa tarkoitetulla tavalla. Turvallisuusluokiteltua asiakirjaa käsitellään aina vastaavan suojaustason mukaisesti. Turvallisuusluokittelu voi perustua myös Suomea sitovaan kansainväliseen sopimukseen tai säädökseen.

Viranomaisen asiakirja: Viranomaisen asiakirjalla tarkoitetaan viranomaisen hallussa olevaa asiakirjaa, jonka viranomainen tai sen palveluksessa oleva on laatinut tai 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 momentti; käsitteen ulkopuolelle jäävistä asiakirjoista, ks. em. lain 5 § 3 ja 4 mom.).

1.7 Tiedon turvallisen käsittelyn muodot ja haasteet, mahdollisuudet ja uhat

Tiedon käsittelyyn liittyy monenlaisia tilanteita. Kun tietoa käsitellään, voidaan puhua tietotyöstä. Kun tietoa talletetaan jälkeenpäin tarkasteltavissa olevaan muotoon, syntyy tallenne. Näitä tallenteita voi syntyä ihmisen välittömän työn tuloksena tai automaattisen järjestelmän tuottamana. Tallenteet kuuluvat julkisuuslain asiakirjan käsitteen piiriin; yksi tallenne saattaa sisältää useita laissa tarkoitettuja asiakirjoja tai vain asiakirjan osan. Esimerkkejä tallenteista ovat mm. tekstinkäsittelyn tuotteet, sähköpostiviestit, tekstiviestit,

äänitallenteet, valokuvat ja videot, tietorekisterien tietokannat, valvontajärjestelmän reaaliaikainen valvontatietoja tietojärjestelmien lokitiedot.

Tiedolla on elinkaari, jonka pituus vaihtelee tiedon ominaisuuden mukaan mikrosekunneista tiedon pysyvään tallettamiseen. Elinkaaren pituudella on välitön vaikutus tiedonhallintaan.

Tietoa tuotetaan ja siirretään yhä enenevässä määrin tietoverkoissa. Avoimissa tietoverkoissa asiakkaina ja käsittelijöinä voivat olla kaikki siellä toimivat. Viranomaisen tietoverkoissa viranomaisella on valta määrätä verkon käyttöön ja tiedon käsittelyyn oikeutetut.

Tietoverkot mahdollistavat tiedon laajan ja nopean käytettävyyden. Tietoverkkoihin liittyy myös suuria uhkia. Näitä ovat esimerkiksi verkkoliikenteen estäminen, väärän informaation tuottaminen eri tietoja yhdistämällä ja tiedon luvaton haltuun ottaminen yksityisyyden suojaa loukkaavalla tavalla.

Viranomaiselta edellytetään tietojen hallintaa. Tiedon hallintaa tarvitaan sekä oman toiminnan tulostavoitteiden saavuttamiseksi että asiakaspalvelun tarpeiden toteuttamiseksi.

2 Asetuksen täytäntöönpanosta

2.1 Ohjaus

Viranomaisen tulee huolehtia hyvän tiedonhallinta- ja tietojenkäsittelytavan toteutumisesta (katso TTA) kehittäessään ja ylläpitäessään tietotyön edellyttämiä järjestelmiä ja palveluja.

Viranomaisen tulee antaa ohjeet viranomaisen palveluksessa oleville henkilöille ja toimeksiannostaan toimiville käsiteltävien asiakirjojen julkisuudesta, tietojen antamisessa ja käsittelyssä noudatettavasta menettelystä sekä asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, turvallisuusjärjestelyistä ja tehtävänjaosta.

Viranomaisen tulee huolehtia, että tietojen käsittelyyn liittyvät prosessit ja niihin liittyvät riskit on arvioitu osana riskienhallintaa.

Viranomaisella tulee olla kuvattuna tiedon koko elinkaarta kuvaava prosessi aliprosesseineen ja näihin liittyvät suunnitelmat erilaisten häiriötilanteiden varalta.

Viranomaisen tulee järjestää teknisten ratkaisujen avulla toimitilojen turvallisuus siten, etteivät ulkopuoliset pääse käsiksi luokiteltuun tietoaineistoon.

Asianhallintajärjestelmien tulee tukea aineiston käytön seurantaa ja arkistointia.

2.2 Koulutus

Viranomaisen tulee antaa tietoaineistojen käsittelyyn osallistuville tarvittava viranomaiskohtainen lisäohjeistus ja koulutus.

Kaikkien suojaustasojen tietojen käsittelyn koulutusta on järjestettävä säännöllisesti ja osana uuden henkilöstön perehdyttämistä.

Viranomaisen tulee kouluttaa tietojärjestelmien suunnitteluun ja toteuttamiseen osallistuva henkilöstö ottamaan huomioon tässä ohjeessa esitetyt vaatimukset hyvän tiedonhallintatavan vaatimusten toteuttamiseksi viranomaisen tarjoamissa tietopalveluissa.

2.3 Valvonta

Viranomaisen tulee valvoa säännönmukaisesti luokiteltujen tietoaineistojen tietoturvatoimenpiteiden toteuttamista sekä seurattava annettujen ohjeiden ja teknisten tietoturvatoimenpiteiden toimivuutta.

Viranomaisen tulee valvoa, että käytössä ovat oikeat työmenetelmät ja henkilöstö toimii kuvatun prosessin mukaisesti eri käsittelytilanteissa.

Henkilötietojen käsittelyä tulee valvoa esim. lokien avulla. Työnantajan on huolehdittava siitä, että valvonnan järjestämisen osalta noudatetaan yksityisyyden suojasta työelämässä annettua lakia (759/2004). Tietojen käytön valvonnan järjestelyistä on ohjeistettu Yleisohje tietoturvallisuuden johtamiseen ja hallintaan -ohjeessa (VAHTI 3/2007) ja lokien käsittelystä annetussa ohjeessa (Lokiohje, VAHTI 3/2009).

Tietoteknisten laitteiden käytöstä poistamisen yhteydessä tai käyttötarkoituksen muuttuessa on huolehdittava jäännöstietojen poistamisesta tehtävään tarkoitetuilla ohjelmistoilla ja kirjattava suoritetut toimet.

Viranomaisen teknisten toimitilojen valvontajärjestelmän toteutuksen on tuettava tietoaineiston suojaamista. Valvontajärjestelmien tietoturvallisuudesta tulee huolehtia vastaavalla tavalla kuin huolehditaan muidenkin tietojärjestelmien tietoturvallisuudesta.

2.4 Seuranta

Viranomaisen tulee ylläpitää tietoaineistojen käsittelyyn liittyvää riskien seurantaa ja esitellä johdolle sovitun aikataulun mukaisesti tietoturvatilanne, minkä tulee sisältää arvio hyvän tiedonhallintatavan toteutumisesta, yhteenveto toteutuneista tietoturvariskeistä, henkilöstölle tarjotusta tietoturvakoulutuksesta ja ohjeistosta sekä viranomaisen tietoturvakulttuurin nykytilasta sekä poikkeamista. Esittelyyn tulee sisällyttää ehdotukset korjaaviksi toimenpiteiksi havaittujen ongelmien osalta.

Sähköisten ja muulla tavoin tallennettujen tietoaineistojen säilytystilat on auditoitava tai tarkastettava säännöllisesti ja niissä olevat poikkeamat korjattava.

Ulkoistetut järjestelmät on hyväksytettävä toimivaltaisella viranomaisella ennen kuin niihin voidaan luovuttaa tietoa, johon kohdistuu suojausvaatimuksia.

2.5 Asetuksen täytäntöönpano

Jokainen viranomainen vastaa tietoturvallisuustasojen toimeenpanosta toiminnoissaan ja yhteistyössään. Tietoturvallisuusasetus määrittää tietoturvallisuustasojen pakolliset vaatimukset. Jokaisen valtionhallinnon viranomaisen

tulee täyttää vähintään tietoturvallisuuden perustaso, joka kattaa kokonaisuudessaan viranomaisen salassa pidettävien asiakirjojen käsittelyn.

Tietoturvallisuuden perustaso tulee olla toteutettuna koko valtionhallinnossa 30.9.2013 mennessä (Tietoturvallisuusasetus 23 § 3 mom.).

Toiminnoissa, joissa edellytetään korotetun tai korkean tietoturvallisuustason toimintaympäristöä (toimintaa, tietojärjestelmiä ja tietoverkkoja) ja joissa käsiteltävät asiakirjat viranomainen on luokitellut, tulee toteuttaa vaatimukset viiden vuoden kuluessa siitä, kun viranomainen on ottanut luokituksen käyttöön.

3 Hyvä tiedonhallinta- ja tiedonkäsittelytapa

3.1 Tiedonhallinnan suunnittelu

Hyvän tiedonhallintatavan toteuttaminen edellyttää viranomaiselta tiedonhallinnan suunnittelua (julkisuuslain 18 §). Suunnittelu alkaa selvittämällä viranomaisen toimintaprosessit. Tällöin on suunniteltava asioihin liittyvät työnkulut, asioiden käsittelyprosessit asiakirjoineen sekä asiakirjojen ja niiden tietojen käyttöoikeudet. Prosessin kuvaus sisältää tiedot siitä

- miten asiat tulevat vireille
- mitä toimenpiteitä käsittelyvaiheisiin liittyy
- miten asiat päätetään
- kuka osallistuu mihinkin prosessin vaiheeseen
- mitä asiakirjoja ja tietoja missäkin vaiheessa syntyy, kertyy tai hankitaan, miten ne talletetaan, rekisteröidään ja säilytetään sekä miten asiakirjoja ja tietoja käsitellään.

Suojaustasoihin I ja II luokitellun tietoaineiston sekä arkaluonteisten henkilötietojen sähköisessä tiedonhallinnassa korostuu aukottoman käsittelyketjun vaatimus, jolloin kaikkien käsittelyvaiheiden on rekisteröidyttävä järjestelmään.

Viranomaisten asiakirjojen käsittely edellyttää arkistonmuodostussuunnitelman olemassaoloa. Tarkemmat ohjeet arkistonmuodostussuunnitelman rakenteesta ja ylläpidosta löytyvät Arkistolaitoksen julkaisusta Arkistonmuodostussuunnitelma AMS (http://www.ams-opas.fi/).

Arkistonmuodostussuunnitelma on viranomaisen asiakirjallisten tietojen käsittelyn, rekisteröinnin ja säilyttämisen ohjeisto. Arkistonmuodostussuunnitelma tuottaa tietojärjestelmiin asiakirjallisen tiedon hallintaan liittyviä metatietoja. Asianhallinnan menettelytavat ja vastuut on kirjattava arkistosääntöön tai johonkin sitä vastaavaan ohjeistoon.

Henkilötietojen käsittely tulee suunnitella henkilötietolain 6 §:ssä edellytetyllä tavalla. Henkilörekisterit tulee tunnistaa ja kartoittaa, niiden käyttötarkoitus tulee määritellä sekä laatia tarvittavat rekisteriselosteet.

Viranomaisen tulee selvittää ja arvioida asiakirjojensa ja niihin sisältyvien tietojen saatavuutta, käytettävyyttä ja suojaamista sekä eheyttä ja muuta tietojen laatua vaarantavat uhkatekijät ja riskit sekä riskien vähentämiseksi käytettävissä olevat keinot, kustannukset ja toimenpiteillä saatavat vaikutukset (julkisuuslaki 18 § 1 mom. 4 k; tietoturvallisuusasetus 4, 5 § 1 mom. 1 k).

Tietojen saatavuuden ja käytettävyyden tavoitteet tulee määritellä toimintojen edellyttämällä tavalla. Tietojen käytettävyyteen vaikuttavat mm. tietoverkon ja tietojärjestelmän ominaisuudet. Erityistä huomiota on kiinnitettävä sovellusten käyttöliittymiin siten, että toiminnon edellyttämät työtehtävät voidaan toteuttaa joustavasti. Tämän edellytyksenä ovat usein nopeat tiedon hakutoiminnot ja toimintaprosessia tukeva toteutus. Tietojen saatavuuden varmistamiseksi tulee suunnitella ja ylläpitää tarvittavia luetteloita (vast.) siten, että niiden avulla mahdollistetaan tiedon välitön hakeminen. Toisaalta näiden avulla tuetaan julkisen tiedon jakamista sitä pyytävälle.

Viranomaisen tulee määritellä ja ohjeistaa menettelyt ja säännöt siitä, miten tuotetaan toiminnasta tietoa julkisuuteen. Käytettäessä internetissä tapahtuvaa tiedottamista tulee varmistaa, että tiedot ovat ajan tasalla ja ylläpidettyjä. Erityistä huomiota tulee kiinnittää myös tietojen eheyden varmistamiseen. On myös muistettava, ettei julkisessa tiedonvälityksessä saa esittää salassa pidettäviä tietoja.

Salassa pidettävän tiedon käsittely tulee suunnitella ja toteuttaa siten, että tietoa voivat käsitellä vain siihen oikeutetut.

Tietojärjestelmien suunnittelussa on otettava huomioon, että hyvän tiedonhallintatavan edellytykset voidaan toteuttaa häiriöttömästi erilaisissa olosuhteissa. Tietojärjestelmien suunnittelussa ja toteutuksessa tulee pyrkiä siihen, että eri prosesseissa tarvittava yhteinen tieto tallennetaan yhteen paikkaan, jota eri prosessit hyödyntävät. Toiminnan varmistamiseen tarvittavat rinnakkaiset järjestelmät tulee suunnitella ja toteuttaa siten, että tietovaranto pysyy eheänä.

Viranomaisen tulee kiinnittää erityistä huomiota tuottamansa tiedon laatuun. Tämä korostuu erityisesti sellaisissa asiakirjoissa ja henkilörekistereissä, joita käytetään yksilöitä ja yhteisöjä koskevassa päätöksenteossa. Laatuvaatimuksissa korostuvat asiakirjojen sisältö, rakenne, allekirjoitukset, jakelut ja aikataulut sekä asiakirjan eheydestä ja kiistämättömyydestä huolehtiminen. Henkilötietolain 9 §:n mukaan rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä.

3.2 Tietoaineiston kartoitus ja hallinta

Viranomaisen on tunnistettava hallussaan olevat asiakirjat (tietovaranto). Näiden tulee pohjautua viranomaisen ylläpitämään arkistonmuodostussuunnitelmaan sekä henkilötietojen osalta henkilötietolain edellyttämään suunnitteluun ja käsittelyn lainmukaisuuden arviointiin.

Viranomaisen on arvioitava riittävän usein asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys samoin kuin käsittelyprosessit.

Arviointityössä tulee julkisuusasetuksen (JulkA) 1 §:n mukaan erityisesti kiinnittää huomio siihen, kuinka toteutetaan:

- oikeus saada tietoja viranomaisen julkisista asiakirjoista
- velvollisuus tuottaa ja jakaa tietoja sekä antaa tietoja keskeneräisistä asioista
- henkilötietojen, erityisesti arkaluonteisten henkilötietojen lainmukainen käsittely ja suojaaminen
- salassa pidettäviksi säädettyjen tietojen suojaaminen
- tietojen käyttötarkoituksia koskevat rajoitukset (henkilötietolain käyttötarkoitussidonnaisuuden vaatimus, muut vaatimukset)
- tietojen suojaus, niiden saanti ja käytettävyys sekä tietojen eheys ja laatu erilaisissa olosuhteissa siten, että viranomaisen tehtävien hoito ja yhteistyö voi sujua häiriöttömästi
- tietojen laatua koskevat vaatimukset erityisesti käytettäessä niitä yksilöitä ja yhteisöjä koskevan päätöksenteon pohjana tai oikeuksien ja velvollisuuksien osoittajina.

Henkilötietojen käsittely tulee suunnitella ja toteuttaa henkilötietolain asettamien vaatimusten pohjalta. Koko käsittelyketju tulee varmistaa siten, että vain tietoon oikeutetut voivat käyttää ja käsitellä tietoja. Lain käyttötarkoitussidonnaisuuden vaatimus merkitsee, että henkilötietoja voidaan käyttää vain siihen tarkoitukseen, johon ne on kerätty. Henkilötietojen käsittelyn tarkoitus on määriteltävä rekisterikohtaisesti. Viranomaisen henkilörekisteristä voidaan luovuttaa henkilötietoja vain säädetyin edellytyksin. (JulkL 16 § 3 mom.)

Henkilörekisteristä tulee laatia ja ylläpitää sekä pitää saatavilla rekisteri- ja tietosuojaseloste.

3.3 Tietoaineistojen luettelointi ja rekisteröinti sekä selosteet

Hyvää tiedonhallintatapaa koskevissa säännöksissä (JulkL 18 § 1 mom. 1 k) määritellään viranomaiselle velvollisuus hallita tietovarantoaan ylläpitämällä asioiden seurantaa varten tarvittavat asiakirjarekisterit ja niiden sisältämät perustiedot. Asiakirjarekistereistä säädetään tarkemmin julkisuusasetuksen luvussa 2.

Viranomaisen on suunniteltava ja ylläpidettävä asiakirjojen rekisteröinnin mahdollistavia rakenteita, joiden avulla mahdollistetaan tietojen suojaaminen sekä niiden käytettävyyden, eheyden ja luotettavuuden varmistaminen.

Julkisuusasetuksessa velvoitetaan viranomaiset laatimaan ja pitämään julkisesti saatavilla selosteet käytössään olevista tietojärjestelmistä. Henkilötietolaissa on säädetty velvoitteesta laatia henkilörekistereistä rekisteriseloste.

Tietoaineistojen luetteloinnin pohjalla tulee olla toimiva ja voimassa oleva arkistonmuodostussuunnitelma. Luettelointitarpeet liittyvät kunkin viraston omaan toimintaan. Luettelointitarpeet tulee tunnistaa ja niiden ylläpito suunnitella asianhallinnan yhteydessä. Automaattisesti toimintaprosessin tuloksena päivittyvien luetteloiden toteuttaminen tulee mahdollisuuksien mukaan ottaa käyttöön.

Osa luetteloista on luonteeltaan erilaisten tapahtumien kirjauksia (esim. lokitiedostot). Nämä sisältävät usein henkilötietoja ja muodostavat henkilörekisterin, jolloin niiden käsittelyyn sisältyy vaatimuksia tiedon käytön ja luovutuksen sekä käsittelyoikeuksien, kiistämättömyyden ja elinkaaren osalta.

3.4 Julkiset ja salassa pidettävät asiakirjat

Julkisuuslaissa määritellään viranomaisten asiakirjat, niiden julkisuus ja salassapitovelvollisuus. Lähtökohdaksi on asetettu viranomaisten asiakirjojen julkisuus. Laissa on erikseen määritelty ne asiakirjat, jotka ovat joko kokonaan tai osittain salassa pidettäviä. Salassapitovelvollisuudesta on säännöksiä myös muissa laeissa.

Julkisiin asiakirjoihin voi asiakirjan merkityksen ja tietosisällön vuoksi liittyä erilaisia käsittelyvaatimuksia. Asiakirjojen tulee olla helposti saatavilla, niin viranomaisten omaa työtä kuin yleisöpalvelua ajatellen. Toisaalta osalle asiakirjoja on asetettu eheysvaatimuksia. Viranomaisen tulee varmistaa, että asiakirjat täyttävät asetetut laatutavoitteet, ovat ajantasaisia ja ovat alkuperäisen asiakirjan mukaisia (asiakirjan informaatio ei ole muuttunut käsittelyvaiheissa).

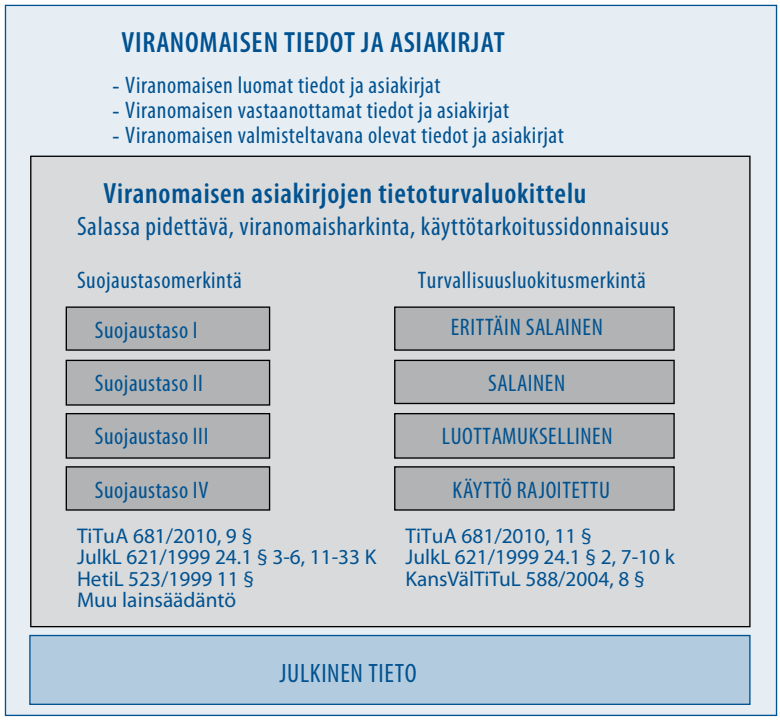
Salassa pidettäviä asiakirjoja saavat käsitellä vain ne henkilöt, joilla on siihen oikeus. Tämä velvoite on voimassa niin kauan, kuin salassapitovelvollisuus on voimassa.

Salassa pidettävän ja tarvittaessa harkinnanvaraisesti julkisen sekä käyttörajoitteisen tietoaineiston käsittelyä ohjataan suojaustasojen avulla tietoturvallisuusasetuksen 9 §:ssä osoitetulla tavalla. Osaan näistä asiakirjoista voidaan tehdä turvallisuusluokittelua koskeva merkintä tietoturvallisuusasetuksen 11 §:ssä säädetyin edellytyksin. Turvallisuusluokitusmerkintää on sallittua käyttää vain niissä tietoaineistoissa, joissa olevien tietojen oikeudeton paljastuminen tai käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille siten kuin tietoturvallisuusasetuksessa säädetään.

Oheisessa kuvassa (kuva 3.1) on esitetty viranomaisten tiedot ja asiakirjat. Osa tästä tietovarannosta kuuluu luokittelun piiriin (keltainen alue). Näiden asiakirjojen ja tietojen käsittelyyn liittyy käsittelyrajoitus. Henkilöllä tulee olla

oikeus niiden käsittelyyn. Osa tästä aineistosta on salassa pidettävää, osa viranomaisharkintaan perustuvaa ja osa käyttötarkoitussidonnan alaista.

Kuva 3.1 Viranomaisen tiedot ja asiakirjat



Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisalan piiriin kuuluva aineisto luokitellaan kansainvälisten velvoitteiden mukaisesti.

On huomattava, että virkamiehen luonnoksiin ja viranomaiselle toimeksiantotehtävän suorittamiseksi annettuihin asiakirjoihin, jotka muutoin jäävät julkisuuslain mukaan viranomaisen asiakirjan käsitteen ulkopuolelle, sovelletaan kuitenkin lain salassapitosäännöksiä (julkisuuslaki, 5 § 5 mom.).

Henkilötiedot eivät yleensä sellaisenaan kuulu luokittelun piiriin. Niiden käsittelylle on asetettu mm. henkilötietolaissa erityisvaatimuksia, kuten käyttötarkoitussidonnaisuus.

Asiakirjarekisteriin, esim. diaariin, merkittyjen tietojen julkisuutta on arvioitava erillään asiakirjojen julkisuudesta. Arviointiin ei vaikuta, ovatko ne asiakirjat, joista viitetiedot viedään rekisteriin, salaisia vai julkisia. Viitetiedot asiasta ja/tai asiakirjoista voivat olla julkisia siitä huolimatta, että itse asiakirjat ovat joko kokonaan tai osittain salassa pidettäviä. Viitetiedot tulee tehdä siten, etteivät ne paljasta salassa pidettävän asiakirjan salassa pidettävää sisältöä.

Viranomaisen on määriteltävä, kenen asiana on ratkaista julkisuuslain nojalla tehdyt pyynnöt saada tieto luokitellusta tai muusta salassa pidettävästä asiakirjasta. Asianmukaisinta on osoittaa tämä tehtävä esimiesasemassa olevalle virkamiehelle, jollei erityisistä syistä muuta johdu.

3.5 Tietoaineistojen saatavuus ja käytettävyys

Viranomaisen tiedon saatavuutta ja käytettävyyttä koskevat vaatimukset riippuvat tiedon merkityksestä viranomaiselle tai siihen oikeutetuille. Monet toimintaprosessit asettavat suuria vaatimuksia oikea-aikaisen ja oikean tiedon saatavuudelle. Julkisuuslaissa määritellään vaatimukset tiedon antamisesta sitä pyytävälle. Saatavuus riippuu esim. tietoverkon ominaisuuksista, varmenteiden käytöstä, tietojärjestelmän käyttöliittymän toteutuksesta, työaseman ominaisuuksista ja käyttäjän osaamisesta.

Julkisten asiakirjojen ollessa kysymyksessä kiinnitetään erityistä huomiota tiedon saatavuudelle ja asian mukaan myös tiedon eheydelle asetettujen vaatimusten toteutumiseen.

Tiedon, tietojärjestelmän tai palvelun on oltava siihen oikeutetun saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditussa ajassa käytettävyysvaatimuksen toteutumiseksi. Lisäksi tulee varmistautua tiedon muuttumattomuudesta ja että tunnistetaan kiistämättömästi asiakirjan muutosvaiheet. Tietojen salassapidosta tai sen käyttörajoitusten toteuttamisesta on huolehdittava siten, että tieto on vain siihen oikeutettujen saatavissa riippumatta siitä, mihin muotoon tieto on talletettu.

3.6 Henkilötietoja koskevat vaatimukset

Henkilötietojen käsittelyä ohjataan mm. seuraavilla säännöksillä

- henkilötietolailla
- julkisuuslain salassapitosäännöksillä sekä tietojen luovuttamista viranomaisen henkilörekisteristä koskevalla julkisuuslain 16.3 §:llä
- hallinnonalakohtaisilla erityislaeilla, joissa on säädetty henkilötietojen käsittelystä.

Henkilörekisterien julkisuutta arvioidaan viranomaistoiminnassa julkisuuslain ja mahdollisten erityislakien mukaisesti. Viranomaisten henkilörekisterit ja niihin sisältyvät tiedot voivat olla julkisuuslain tarkoittamalla tavalla julkisia tai ne voivat olla lain 24 §:n tai muun lain nojalla salassa pidettäviä.

Henkilötietojen käsittelyssä ja henkilörekisterin perustamisessa on otettava huomioon henkilötietolain säännökset. Henkilötietolakia sovelletaan henki-

lötietojen automaattiseen käsittelyyn. Myös muuhun käsittelyyn sovelletaan henkilötietolakia silloin kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa.

Henkilörekisterin perustamisen ja siihen talletettujen henkilötietojen käsittelyn tulee olla viranomaisen toiminnan kannalta perusteltua. Henkilötietojen käsittely tulee suunnitella koko elinkaaren ajan. Henkilörekisterit ja niiden tiedot tulee suojata siten, että ne ovat vain tietoon oikeutettujen käsiteltävissä. Talletettujen henkilötietojen tulee olla virheettömiä, mikä asettaa vaatimuksen tietojen ylläpidolle. Vain käyttötarkoituksen kannalta tarpeellisia ja virheettömiä tietoja saa kerätä, tallettaa ja muutoin käsitellä. Lisäksi tulee ottaa huomioon rekisteröityjen oikeuksien toteutus: rekisteröityjen informointi sekä tarkastusoikeuden ja tiedon korjaamista koskevien pyyntöjen käsittely.

Henkilötietolain 7 §:n mukaan henkilötietoja saa käyttää tai muutoin käsitellä pääsääntöisesti vain tavalla, joka on yhteensopiva lain 6 §:ssä tarkoitettujen käsittelytarkoitusten kannalta. Henkilörekisterin tietoja saa käyttää vain niihin käyttötarkoituksiin, jotka on määritelty rekisteriä perustettaessa.

Suojaamisvelvoitteet on arvioitava henkilörekisterikohtaisesti. Henkilötietolain 32 §:n mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

Arkaluonteisia henkilötietoja ei saa käsitellä muutoin kuin henkilötietolain 12 §:ssä tarkoitetuilla edellytyksillä ja tilanteissa. Arkaluonteiset tiedot ovat yleensä salassa pidettäviä. Tietoturvallisuusasetukseen sisältyy eräitä luokiteltujen arkaluonteisten henkilörekisteriin talletettujen henkilötietojen käsittelyä koskevia velvoitteita, jotka eivät ole riippuvaisia siitä, onko tiedot säädettysäädetty salassa pidettäviksi vai ei (ks. tietoturvallisuusasetus 13 § 1 mom., 14 § 4 k, 16 § 3 mom.19 § 3 mom., 20 § 1 mom.).

4 Tietojenkäsittelyn yleiset tietoturvavaatimukset

Tässä luvussa esitetään tietojenkäsittelylle asetettavia yleisiä vaatimuksia. Näitä ovat mm. henkilöstön osaamisen ja luotettavuuden varmistaminen sekä tietojenkäsittely-ympäristöille asetettujen vaatimusten täyttäminen.

Tietoturvallisuuden tarkoituksena on varmistaa viranomaisen toiminnan jatkuvuus ja laatu sekä oikeusturvan toteutuminen. Tietoturvallisuuden toteuttaminen perustuu omien tietoaineistojen ja niiden merkityksen sekä tietoturvariskien kartoitukseen.

Viranomaisen on huolehdittava kaikessa suunnittelussa ja toimeenpanossa, että henkilöstön käytössä ovat turvalliset työvälineet, tilat ja toiminnot ja että henkilöstö on tietoinen tietotyön riskeistä, tuntee oikeat menettelytavat ja on myötävaikuttamassa omalla asenteellaan korkean tietoturvakulttuurin olemassaoloon.

Tietoturvallisuuden johtaminen ja hallinta on ohjeistettu ohjeessa Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007).

4.1 Tietoturvallisuusasetuksen yleiset tietoturvavaatimukset

Viranomaisen on toteutettava ja ylläpidettävä vähintään tietoturvallisuuden perustason vaatimukset täyttävää tiedonkäsittely-ympäristöä toimintansa edellyttämässä laajuudessa.

Viranomaisen on huolehdittava siitä, että sen käytössä on riittävä osaaminen tietoturvatehtävien tarpeen arvioimiseksi, toimenpiteiden toteuttamiseksi, kehittämiseksi ja valvomiseksi sekä ohjauksen antamiseksi henkilöstölle.

Tietoturvallisuusasetuksen (TTA 8 §) mukaan viranomainen päättää, otetaanko virastossa käyttöön asiakirjojen luokitus. Jos luokitukseen päädytään, luokittelussa ja asiakirjojen käsittelyssä on noudatettava asetuksen lukuja 3 ja 4. Vaikka viranomainen ei luokittelekaan asiakirjoja, sen on noudatettava julkisuuslain 18 §:ssä ja tietoturvallisuusasetuksen luvussa 2 säädettyjä velvoitteita.

Säännöksissä edellytetään, että viranomainen selvittää ja arvioi asiakirjansa ja tietojärjestelmänsä sekä toimintaansa liittyvät tietoturvariskit (JulkL 18 §,

JulkA 1 §, TTA 4 §, 5 § 1 mom. 1 k). Hyvän tiedonhallintatavan edellytysten luominen viranomaisessa merkitsee erityisesti asiakirjojen ja tietoaineistojen saatavuudesta ja käytettävyydestä huolehtimista. Hyvään tiedonhallintatapaan kuuluu myös huolehtia rekisteröintitietojen, asioiden ja asiakirjojen hyvästä julkisuus- ja salassapitorakenteesta sekä salassa pidettäväksi säädettyjen tietojen suojaamisesta. Henkilötietolaki edellyttää hyvän tietojenkäsittelytavan toteuttamista henkilötietojen käsittelyssä.

Viranomaisen on määriteltävä asiakirjojen ja tietojen käsittelyyn liittyvät tehtävät ja vastuut (5 § 1 mom. 3 k). Se, kenellä on toimivalta päättää salassa pidettävien asiakirjojen tai henkilötietojen luovuttamisesta tai oikeus käsitellä tällaisia tietoja, on määriteltävä sisäisin määräyksin, jollei asiasta ole säädetty.

Tietojen suojaamiseksi tarpeelliset toimenpiteet on toteutettava niin perinteisessä asiakirjahallinnossa kuin tietojärjestelmissä tietoturvallisuuden perustason varmistamiseksi. Tietojärjestelmissä tulee toteuttaa asianmukainen käyttövaltuushallinta ja käytön valvonta sekä huolehtia riittävistä tietoverkkojen ja tietojärjestelmien turvallisuusjärjestelyistä (5 § 1 mom. 6 k). Järjestelmien toimivuus ja tietojen saanti tulee turvata eri tilanteissa (5 § 1 mom. 4 k).

Tilat, joissa salassa pidettäviä tietoja ja henkilörekistereitä käsitellään, tulee olla asianmukaisesti suojattuja, valvottuja ja tähän käyttöön hyväksyttyjä (5 § 1 mom. 7 k).

Henkilöstön luotettavuuden selvittämisessä käytetään tarvittaessa turvallisuusselvityksiä ja muita lain perusteella käytettävissä olevia keinoja (5 §1 mom. 8 k).

Henkilöstölle annetaan tarvittavat tietoturvallisuutta koskevat ohjeet, joita valvotaan ja pidetään ajan tasalla (5 § 1 mom. 9 k).

Tässä ohjeessa annetaan ohjeita salassa pidettävien asiakirjojen käsittelystä suojaustasojen määrittelemiseksi, salassapitomerkinnän ja turvallisuusluokkamerkintöjen tekemiseksi sekä tietoturvallisuustasojen määrittelemiseksi.

4.2 Henkilöstöä koskevat vaatimukset

Salassa pidettäviä asiakirjoja tai henkilörekisteriin talletettuja henkilötietoja saavat käsitellä vain ne henkilöt, joilla on oikeus kyseisten asiakirjojen käyttöön. Käsittelyoikeuden saaminen edellyttää, että

- henkilöllä tulee olla esimiehen määrittämä, työtehtäviin liittyvä tarve käsitellä asiakirjan sisältämää tietoa
- henkilön tulee tuntea ja hallita salassa pidettävien asiakirjojen käsittelysäännöt
- henkilön luotettavuus on tarvittaessa selvitetty asiaan kuuluvalla tavalla, esim. turvallisuusselvitysmenettelyn avulla. Tämä vaatimus koskee erityisesti suojaustasoa I ja II edellyttävän tietoaineiston käsittelyä

- henkilöllä tulee olla voimassa oleva käsittelyoikeus käsitellä asiakirjassa määritellyn suojaustason mukaista tietoa. Tämä vaatimus koskee erityisesti suojaustasoa I ja II edellyttävän tietoaineiston sekä turvallisuusluokkien I – III mukaisen tiedon käsittelyä.

Käsittelyoikeus tulee sitoa työtehtävään. Henkilöllä tulee olla pääsy työtehtäviensä edellyttämiin tietoihin ja asiakirjoihin. Kun henkilön oikeus salassa pidettävän aineiston hallussa pitämiseen muuttuu, tulee henkilöltä poistaa käyttövaltuushallinnan menetelmin käyttöoikeudet kyseiseen aineistoon ja henkilön tulee luovuttaa pois hallussaan oleva salassa pidettävä tietoaineisto tai tuhota se viranomaisen johdon määrittelemällä tavalla. Salassa pidettäviä asiakirjoja tulee käsitellä huolella siten, että vain käyttöoikeuden omaavat pääsevät käsiksi salassa pidettävään tietoon.

Henkilöstön tulee tuntea ja hallita tietojen käsittelyssä tarvittavien työvälineiden turvallisuusmenettelyt. Henkilöstölle tulee antaa määrävälein ja aina muutosten yhteydessä tarvittavaa koulutusta ja varoittaa havaituista vaaroista.

Viranomaisen tulee ylläpitää tehtäväluetteloa omasta henkilökunnastaan, eli tietoa siitä, kuka saa missäkin työtehtävässä käsitellä salassa pidettäviä asiakirjoja tai henkilörekisteriin kuuluvia henkilötietoja. Työtehtävään kuuluvat tyypilliset tietovarantojen käsittelytarpeet voidaan kuvata tehtäväkuvauksen yhteydessä. III ja IV luokissa on jokaisella virkamiehellä oikeus käsitellä tietoa työtehtäviensä tarpeiden mukaisesti viranomaisen johdon päätöksiin perustuen (Tietoturvallisuusasetus 13 §). Kansainvälisten tietoturvavelvoitteiden toteuttaminen edellyttää yleensä henkilötasoista tietojen käyttöoikeusluetteloa ja sen ylläpitoa.

Yksityiskohtaiset ohjeet suojaustasoittain on esitetty liitteen 3 luvussa 2.

Viranomainen voi edellyttää, että sen palveluksessa oleva henkilöstö tarvittavassa laajuudessa on läpäissyt tietoturvallisuuden osaamistestin.

4.3 Tietoturvakulttuurin perusedellytyksiä

Viranomaisen tulee ylläpitää koko henkilökunnalle tarkoitettua tietoturvakoulutusta ja varmistua henkilöstön riittävästä osaamisesta ja tietoturvallisuuteen liittyvien riskien ymmärtämisestä.

Henkilöstön tulee tuntea riittävässä määrin viranomaisen tietoturvapolitiikka ja tietoturvatoimintaa käsittelevä ohjeisto

Henkilöstön tulee olla sitoutunut noudattamaan annettuja tietoturvaohjeita.

Kaikkien salassa pidettävien ja luokiteltujen asiakirjojen käsittelyyn osallistuvien tulee tiedostaa, että organisaation oma henkilöstö aiheuttaa valtaosan tietoturvaongelmista. Syyt tapahtumiin ovat moninaiset. Yhtenä yhdistävänä tekijänä on yleensä huolimattomuus tietoaineiston tai työvälineen käytössä. Toinen yleinen syy liittyy piittaamattomuuteen annettujen ohjeiden noudattamisesta. Kolmas syy on, ettei henkilölle ole annettu riittävää koulutusta tai ohjeistusta.

4.4 Tilaturvallisuutta koskevat vaatimukset

Tilaturvallisuuden tarkoituksena on osana fyysistä turvallisuutta suojata henkilöstöä, tietoa ja materiaalia. Tilaturvallisuudella tarkoitetaan kaikkia niitä rakenteellisia ja valvonnallisia järjestelyjä, joilla varmistetaan tilojen pysyminen vain oikeutettujen hallinnassa ja käytössä sekä käyttötarkoituksen edellyttämässä kunnossa. Rakenteilla tarkoitetaan seiniä, kattoja, ikkunoita, ovia, paloturva- ja kassakaappeja sekä muita mekaanisia ratkaisuja. Valvontajärjestelmillä tarkoitetaan yleensä kulunvalvonta-, tunkeutumisen ilmaisu-, kameravalvonta- ja olosuhdevaroitusjärjestelmiä. Sähköisiin valvontajärjestelmiin kuuluvat myös kiinteistöautomaatiojärjestelmät, joilla valvotaan ja ohjataan tilan käyttöolosuhteita.

Tilaturvallisuuden kokonaisuudesta ei ole olemassa varsinaisia standardeja, mutta kunkin tietoturvallisuustason mukaiset viranomaisvaatimukset on esitetty yksityiskohtaisesti Kansallisen turvallisuusauditointikriteeristön (KATAKRI) fyysisen turvallisuuden osiossa.

Viranomaisen on määriteltävä vastuullaan olevien tilojen turvallisuusratkaisut. Määrittelyssä on huomioitava mm. rakenteelliset ratkaisut, tarvittavat valvontajärjestelmät ja mahdollisesti tilojen käyttöoikeuksiin liittyviä asioita.

Tilaturvallisuutta tulee tarkastella kokonaisuutena. Kokonaisuuteen kuuluvat esim. tietoverkkojen laite- ja ristikytkentätilojen tilaturvallisuuden huomioiminen sekä huolehtiminen siitä, etteivät asiattomat pääse käsiksi mm. aktiivisiin kytkentärasioihin.

Valvontajärjestelmillä valvotaan kulkua tiloihin ja havaitaan asiaton liikkuminen niissä. Valvontajärjestelmät ovat tietojärjestelmiä. Valvontajärjestelmät tuottavat usein henkilörekistereitä. Videovalvonnassa työpaikalla on noudatettava, mitä laissa yksityisyyden suojasta työelämässä (759/2004) säädetään.

Valvontajärjestelmien tietoturvallisuudesta tulee huolehtia vastaavalla tavalla kuin huolehditaan muidenkin tietojärjestelmien tietoturvallisuudesta.

Kiinteistöautomaatiojärjestelmien tietoturvallisuuden tulee olla asianmukaista ja erityisesti käyttöoikeuksien hallinnan on oltava valvottua. Kiinteistöautomaatiojärjestelmillä huolehditaan laitetilojen käyttöolosuhteista ja vaikuttamalla niihin voidaan tietojärjestelmien palvelut romahduttaa. Kiinteistöautomaatiojärjestelmiä voidaan usein etävalvoa, jolloin olosuhteiden muuttaminen voi tapahtua viranomaisen ulottumattomista.

Tilaturvallisuudessa on otettava huomioon myös tilojen äänieristys. Äänieristys on huomioitava kaikissa niissä tiloissa, joissa käsitellään salassa pidettävää tietoa. Erityistä huomiota on kiinnitettävä kaapelien läpivienteihin ja ilmanvaihtojärjestelmän kautta kulkevan äänen eristämiseen.

Tilaturvallisuudessa on otettava huomioon myös sähkömagneettisesta hajasäteilystä syntyvä uhka erikseen määriteltävissä tapauksissa toimivaltaisen viranomaisen määrittämässä laajuudessa (Tempest-suojaukset).

Organisaatiolla on vastuu siitä, että tiedon käsittelyyn käytetyt tilat ovat asianmukaisesti suojatut. Tilan käyttäjällä tulee olla tieto kyseisen paikan tilaluokasta (turvallisuusvyöhykkeestä), erityisesti käsiteltäessä salassa pidettävää tietoa.

Arkistolaitos on ohjeistanut arkistotilojen vaatimukset.

Yksityiskohtaiset ohjeet suojaustasoittain on esitetty liitteen 3 luvussa 4.

5 Tietoteknistä ympäristöä koskevia tietoturvavaatimuksia

5.1 Tietoteknistä ympäristöä ja tietopalveluja koskevia vaatimuksia

Tietoaineistojen käsittelyssä käytettävät tietoverkot ja tietojärjestelmät tulee toteuttaa siten, että ne mahdollistavat tietotyön turvallisen toteuttamisen kaikissa tilanteissa.

Tietoverkkojen ja tietojärjestelmien sisältämät laitteet ja komponentit tulee sijoittaa turvallisiin tiloihin (Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002). Järjestelmät tulee rakentaa siten, että toiminnan edellyttämä tietotyö voidaan suorittaa asetettujen käytettävyysvaatimusten mukaisesti.

Tietotekniset ympäristöt luokitellaan tietoturvallisuustasojen avulla. Viranomaisen tulee toteuttaa vähintään perusturvatason toimintaympäristö.

Tietojärjestelmän ja tietoverkon, jossa käsitellään salassa pidettävää tietoa, tulee täyttää kyseisen tiedon suojaustasolle asetetut vaatimukset.

Tietoverkon ja tietovarantojen sekä toimitilojen käyttöä tulee valvoa.

Viranomaisen tulee huolehtia siitä, että tietoaineiston käsittelyyn tarkoitetut työvälineet ja järjestelmät sisältävät tarvittavat turvallisuusjärjestelyt, esim. haittaohjelmien torjuntajärjestelmät ja tietoaineistojen salausmenettelyt sekä käyttöoikeuksien hallintamenettelyt.

Luokiteltua tietoa sisältävän työaseman käyttö tulee olla mahdollista vain käyttöoikeuden varmistavin järjestelyin.

Tiedonkäsittely-ympäristöt tulee suojata riittävästi hajasäteilyn osalta.

Viranomaisen on määriteltävä, kenen asiana on ratkaista julkisuuslain nojalla tehdyt pyynnöt saada tieto luokitellusta asiakirjasta. Asianmukaisinta on osoittaa tämä tehtävä esimiesasemassa olevalle virkamiehelle, jollei erityisistä syistä muuta johdu.

Yksityiskohtaiset ohjeet on esitetty liitteen 3 luvussa 5.

5.2 Sidosryhmien käyttö tietoteknisten järjestelmien ja palvelujen toimittajana ja ylläpitäjänä

Yhteistoimintaa sidosryhmien kanssa säätelee kansallinen lainsäädäntö. Muun muassa perustuslaki, julkisuuslaki, henkilötietolaki ja sähköisen viestinnän tietosuojalaki sekä tietoturvallisuusasetus asettavat vaatimuksia, jotka on otettava huomioon käytettäessä ulkopuolisia organisaatioita osana viranomaistehtävien hoitamista. Tällaisia ovat esim. tietosuojaan ja varautumiseen liittyvät sijaintirajoitteet.

Tietoteknisten järjestelmien ja palvelujen kehittämiseen ja ylläpitoon liittyy useilla viranomaisilla turvallisuusluokiteltavan tietovarannon käsittelytehtäviä. Tästä syystä toimeksiannot tulee suunnitella etukäteen huolella ja varmistua toimittajien kyvystä suojata heidän käyttöönsä annettavaa luokiteltua tietovarantoa.

Toimeksiannot tulisi tehdä sellaisten yritysten kanssa, joilla on Suomessa riittävän vahvat toiminnot ja tuki toimeksiannon kannalta.

Mikäli hankintaan tai palveluun liittyy luokiteltavan tietovarannon käsittelyä, tulee toimittajan kanssa varmistua etukäteen turvallisuusjärjestelyistä. Mikäli kyse on ulkomaisista toimijoista ja henkilöistä, tulee kääntyä kansallisen turvallisuusviranomaisen puoleen ja pyytää tätä selvittämään kyseisen toimijan ja henkilöstön osalta tarvittavat turvallisuustiedot.

Ensimmäinen ehdotus Kansalliseksi turvallisuusauditointikriteeristöksi (KATAKRI) valmistui vuonna 2009 viranomaisten, elinkeinoelämän sekä turvallisuusalan järjestöjen yhteistyönä. Kriteeristöllä ei toistaiseksi ole ohjeluonnetta ja sen päätavoitteena on auttaa yrityksiä ja muita yksityisiä yhteisöjä sisäisessä turvallisuustyössään. Se sisältää kuitenkin suosituksia, joihin on hyvä tutustua suunniteltaessa viranomaisten tietoturvallisuustoimia.

Tässä yhteydessä tulee ottaa huomioon valtioneuvoston huoltovarmuuden tavoitteista antama päätös (539/2008), jonka mukaan yhteiskunnan toimivuudelle kriittisiä tietojärjestelmiä suunniteltaessa ja rakennettaessa on varmistettava, että niihin liittyvän ohjauksen, ylläpidon, järjestelmähallinnan ja teknisen tuen osaaminen säilyy Suomessa tai että ohjaus- ja hallintakyky on mahdollista palauttaa Suomeen. Päätöksessä edellytetään, että keskeisten sovellusten käyttämien tietovarantojen tulee olla Suomessa.

5.3 Tietoturvallisuustasojen perusteet

Tietoteknisten ympäristöjen ja niiden hallintaa varten määritellään valtionhallinnossa seuraavat tietoturvallisuustasot:

- Tietoturvallisuuden perustason ympäristö (perustaso)
- Korotetun tietoturvallisuustason ympäristö (korotettu taso)
- Korkean tietoturvallisuustason ympäristö (korkea taso).

Tietoturvallisuusasetuksessa asetetaan valtionhallinnon viranomaisille vaatimus täyttää vähintään tietoturvallisuuden perustaso.

Perustason ympäristö mahdollistaa suojaustasoa IV sisältävien tietojen ja asiakirjojen käsittelyn selväkielisessä muodossa.

Korotetun tietoturvallisuustason ympäristö mahdollistaa suojaustasoa III (sisältävien tietojen ja asiakirjojen käsittelyn selväkielisessä muodossa (tietoturvallisuusasetus, 16 § 3 mom.).

Korkean tietoturvallisuustason ympäristö mahdollistaa suojaustasoa II sisältävien tietojen ja asiakirjojen käsittelyn selväkielisessä muodossa (tietoturvallisuusasetus 16 § 2 mom.).

Suojaustasoa I sisältävien tietojen selväkielinen käsittely voidaan toteuttaa vain erillisverkkoympäristöissä, joissa ei ole liitäntöjä alemman tietoturvallisuustason ympäristöön.

Tiedonkäsittelyyn käytettävien laitteiden (työasemien, vast) tulee täyttää kyseiselle tietoturvallisuustasolle asetetut vaatimukset.

Työasema, joka itsessään täyttää korkeamman tietoturvallisuustason vaatimukset, on mahdollista erilliseen viranomaishyväksyntään perustuen liittää alemman tietoturvallisuustason ympäristöön.

Yksityiskohtaisemmat ohjeet eri turvallisuustasoille asetetuista vaatimuksista on esitetty liitteessä 5.

5.4 Tietoturvallisuustasojen asettamiseen liittyvät tavoitteet

Tietoturvallisuustasojen avulla asetetaan vaatimukset sekä teknisten turvallisuusjärjestelyjen että hallinnollisten menettelyjen toteuttamiseksi ja ylläpitämiseksi tietojenkäsittely-ympäristöissä. Mitä korkeamman tietoturvallisuustason ympäristö täyttää, sitä paremmat mahdollisuudet se tarjoaa eri suojaustasoihin kuuluvan tietovarannon käsittelyyn.

Toteutettava tietoturvallisuustaso kussakin toimintaympäristössä tulee määrittää toimintaprosessien ja niissä käsiteltävien tietojen sisällön ja merkityksen sekä niihin kohdistuvien uhkien ja riskien pohjalta.

Kun tunnetaan tiedonkäsittely-ympäristön tietoturvallisuustaso, voidaan kyseisessä ympäristössä tapahtuva tietojen käsittely toteuttaa yhtenäisten käsittelysääntöjen pohjalta (liite 4).

Tietoturvallisuustasojen avulla lisätään mahdollisuutta salassa pidettävien tietojen vaihtoon eri viranomaisten ja viranomaisille palveluja tuottavien sidosryhmien kesken. Tietojenkäsittely-ympäristöt ja toiminnot tulee arvioida asetettuja vaatimuksia vastaan (luku 5.6 ja liite 5.1 luku 6).

Viranomaisen tulee päättää, mikä on tietoturvallisuuden rooli organisaation keskeisten tehtävien suorittamisessa, millä resursseilla se saadaan aikaan ja millaisten uhkien torjuntaan nämä resurssit on ensisijaisesti suunnattava. Täl-

laisilla ohjausmekanismeilla johto voi varmistua siitä, että tietoturvallisuuden vuoksi tehtävä panostus kohdistuu toiminnan kannalta oikeisiin kohteisiin ja tietoturvallisuustaso on mitoitettu oikein toimintaan nähden. Toimivat ohjausmekanismit ovat avuksi riittävän tietoturvallisuuden tason saavuttamisessa.

Viranomaisessa voi olla eri tietoturvallisuustasojen osatoimintoja, tietojärjestelmiä ja tietoverkkoja. Osituksen lähtökohtana tulee olla riskiarviointien ja kustannustehokkuuden yhteensovittaminen.

5.5 Suojattavat kohteet ja tekniset suojausmekanismit

Eräs tietoturvallisuuden kehittämisen keskeisistä tehtävistä on tunnistaa organisaation suojattavat kohteet. Näitä ovat esim, suojattavat tietoaineistot, työasemat, ja tietojärjestelmät sekä niiden tilat, samoin kuin tietoverkot.

Kehittämistyön pohjalla tulee olla jatkuva riskien arviointi. Tulee tunnistaa tietoihin ja tietopalveluihin liittyvät riskit sekä luoda näiden hallitsemiseksi organisaation toimintaan sopivat käsittelymenetelmät. Keinot voivat olla erilaisia; koulutuksista, ohjeistuksista ja sopimuksista teknisiin ohjelmistoihin ja menetelmiin.

Yksittäisten korotetun tai korkean tason vaatimusten käyttö voidaan organisaatiossa katsoa tarpeelliseksi jo alemmilla tasoilla. Mahdollisista suojauskeinoista löytyy paljon tietoa valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) julkaisemista ohjeista.

5.6 Tietoturvallisuustason määrittely ja arviointi

Viranomaisen on arvioitava tiedon käsittelyyn käyttämiensä ympäristöjen tietoturvallisuustaso. Tämä voidaan suorittaa itsearviointimenetelmää tai ulkoista arviointia käyttämällä. Apuvälineenä tähän voi käyttää VAHTI-ohjeistoa sekä Valtion IT-palvelukeskuksen tarjoamia välineitä.

Perusvaatimuksena on, että kukin tiedonkäsittely-ympäristö sekä hallinnolliset toiminnot täyttävät tietoturvallisuuden perustasolle asetetut vaatimukset. Tämä koskee sekä viranomaisen omia järjestelyjä että niitä tahoja, jotka suorittavat tehtäviä viranomaisen toimeksiannosta.

Valtionhallinnon viranomaisten toiminnassa tulisi lähtökohtana olla, että käsiteltäessä yhteiskunnan elintärkeiden toimintojen kannalta kriittisiä viranomaisen asiakirjoja, käsittelyssä noudatetaan joko korotetun tai korkean tietoturvallisuustason vaatimuksia.

6 Hallinnollista tietoturvallisuutta koskevia vaatimuksia

6.1 Tietoturvallisuuden kehittäminen

Viranomaisen tulee kehittää ja ylläpitää tietoturvallisuuden hallintajärjestelmää, joka rakentuu viranomaiselle asetettujen tehtävien toteuttamisen mahdollistamiseksi hyvää tiedonhallintatapaa noudattaen. Tietoturvallisuuden hallinta tulee sitoa organisaation muuhun johtamis- ja kehittämismalliin.

Valtionhallinnossa tietoturvallisuuden johtamisen ja hallinnan perustana ovat lainsäädäntö ja VAHTI-ohjeet. Tietoturvallisuuden hallintajärjestelmän kuvaus on esitetty VAHTI-ohjeessa 3/2007.

6.2 Tietoturvallisuuden hallinnan vaatimukset

Tietoturvallisuuden hallintaa käsitellään tässä asiakirjassa seuraavien, CAF-laatumallista johdettujen osatoimintojen avulla:

- Johtajuus
- Strategiat ja toiminnan suunnittelu
- Henkilöstö
- Kumppanuudet ja resurssit
- Toiminnan prosessit
- Mittaaminen.

Johtajuus sisältää seuraavat alakohdat:

- Strateginen ohjaus
- Resursointi ja organisointi
- Yhteistyön koordinointi
- Raportointi ja viestintä sidosryhmille
- Johtaminen erityistilanteissa
- Raportointi johdolle.

Tietoturvallisuuden strategian määrittelyssä ja toiminnan suunnittelussa voidaan tunnistaa seuraavat alakohdat:

- Toimintaympäristön vaikutus
- Tavoitteiden määrittely
- Toiminnan kehittäminen riskien arvioinnilla
- Toimintaverkoston hallinta
- Erityistilanteiden hallinta.

Tietoturvallisuuden henkilöstöhallinnassa voidaan erottaa seuraavat alakohdat:

- Osaamisen ja tietoisuuden kehittäminen ja sanktiot
- Henkilöresurssien ja tehtävien hallinta
- Erityistilanteissa toimiminen.

Kumppanuuksien ja resurssien hallinta voidaan jakaa seuraaviin alakohtiin:

- Sopimusten hallinta
- Toiminnan varmistaminen erityistilanteissa.

Tietoturvallisuuden toimintaprosesseilla ymmärretään tässä kaikkia niitä prosesseja, joissa käsitellään tietoa ja tietopalvelua. Näitä käsitellään alakohdassa

- Tietoaineistojen hallinta.

Tietoturvallisuuden mittaaminen eli arviointi tarkoittaa niitä toimenpiteitä, joiden avulla varmistutaan nykytilanteen toimintojen tasosta. Ne käsitellään alakohdassa

- Toiminnan arviointi ja todentaminen.

Tietoturvallisuuden hallintajärjestelmän avulla varmistetaan tietoturvallisuuden toteutuminen kaikissa toimintaprosesseissa. Hallintajärjestelmän avulla seurataan prosessien nykytilaa ja mahdollisia ongelmia sekä ohjataan korjaavien toimenpiteiden toteutumista. Hallintajärjestelmän avulla ohjataan myös tietojärjestelmien ja palvelujen kehittämistyötä tietoturvallisuuden vaatimusten osalta.

Kullekin tietoturvallisuustason ympäristölle tulee asettaa sekä hallinnolliset että tekniset vaatimukset edellä esitettyjen alakohtien osalta.

Liitteessä 5 on esitetty yksityiskohtaiset vaatimukset tietoturvallisuuden hallinnalle eri tietoturvallisuustasojen osalta. Pääosa yksityiskohtaisista vaatimuksista on muodostettu VAHTI-ohjeiden sisällöstä.

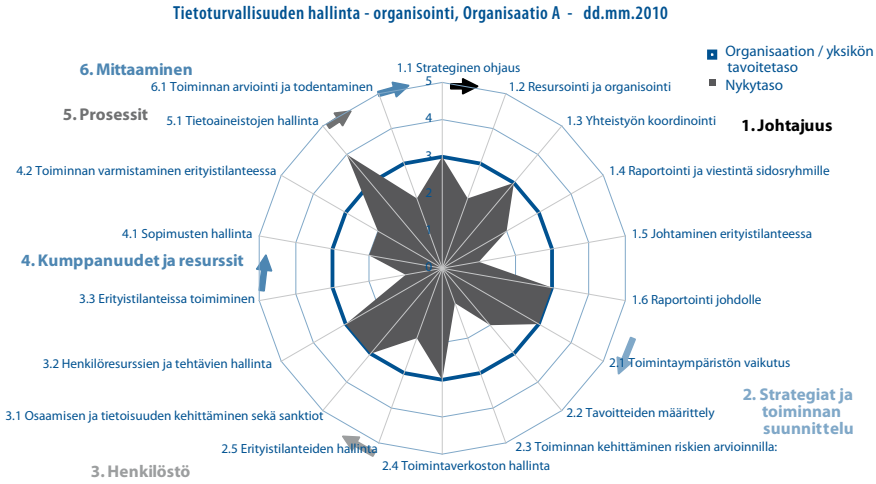
6.3 Tietoturvallisuuden hallinnan arviointi

Viranomaisen tulee ylläpitää riittävän kattavaa seurantajärjestelmää tietoturvallisuuden eri osa-alueiden tilanteen arvioimiseksi.

Viranomaisen tulee laatia määräajoin seurantaraportti tietoturvallisuuden tilasta ja esitellä se ylimmälle johdolle johdon katselmuksissa.

Seurantaraportin tulee sisältää oheisen kuvan (kuva 6.1) mukainen tulos, jossa kunkin käsiteltävän asian osalta nähdään asetettu tavoite ja arvio nykytilanteesta.

Kuva 6.1 Esimerkki tarkasteltavan tietojenkäsittely-ympäristön tietoturvallisuuden hallinnan tavoitetilasta sekä arviointiin pohjautuvasta nykytilasta.



Ylimmän johdon tulee tiedostaa olemassa olevat kriittiset riskit ja päättää korjaavista toimenpiteistä.

6.4 Tietojärjestelmien ja tietopalvelujen hallinnan vaatimukset

Viranomaisen on ylläpidettävä omaan toimintaan mitoitettua ja riittävän tehokasta tietojärjestelmien ja tietopalvelujen hallintaa.

Hallinnan tulee sisältää toimivat menettelyt mm. seuraavista osa-alueista:

- 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
- Tietojärjestelmien toipuminen häiriötilanteista
- Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta.

Tietojärjestelmien ja tietopalvelujen hallinta edellyttää riittävien ylläpitoresurssien olemassaoloa. Tämä tarve korostuu niissä ympäristöissä, jotka ovat jatkuvan kehityksen kohteena ja joiden avulla mahdollistetaan viranomaisen ydintoiminnot.

Toiminnan tulee sisältää jäljitettävissä olevat prosessit, joiden avulla voidaan todentaa tietojenkäsittely-ympäristöjen, tietojärjestelmien ja muiden tietoturvallisuuden tilaa kuvaavat toiminnot ja niiden muutokset

Liitteessä 5 on esitetty tietojärjestelmien ja palvelujen hallintaa koskevat yksityiskohtaiset vaatimukset.

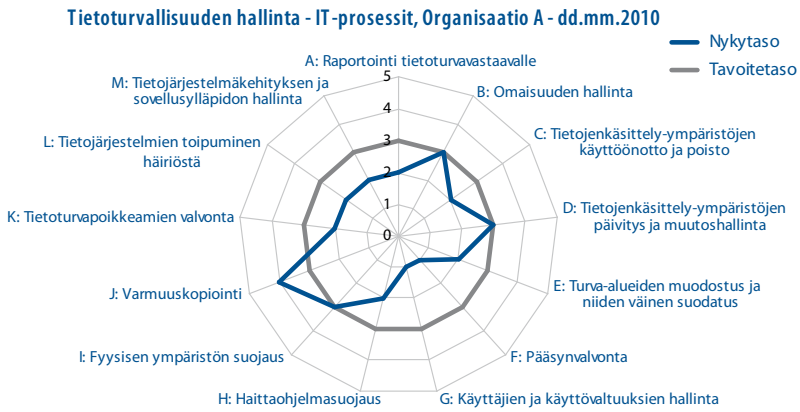
6.5 Tietojärjestelmien hallinnan arviointi

Viranomaisen tulee ylläpitää riittävän kattavaa seurantajärjestelmää tietojärjestelmien hallinnan osa-alueiden tilanteen arvioimiseksi.

Viranomaisen tulee laatia määräajoin seurantaraportti tietojärjestelmien hallinnan tilasta ja esitellä se ylimmälle johdolle johdon katselmuksissa.

Seurantaraportin tulee sisältää oheisen kuvan (kuva 6.2) mukainen tulos, jossa kunkin käsiteltävän asian osalta nähdään asetettu tavoite ja arvio nykytilanteesta.

Kuva 6.2 Esimerkki tietoteknisen ympäristön hallintaa kuvaavasta tavoitetilasta sekä arvioinnin pohjalle rakentuvasta nykytilasta.



Ylimmän johdon tulee tietää olemassa olevat kriittiset riskit ja päättää korjaavista toimenpiteistä.

7 Tietoaineistojen luokittelu

Julkisuuslaki asettaa viranomaiselle velvoitteet hallita käytössään olevia tietovarantoja hyvän tiedonhallintatavan mukaisesti. Tietovarantojen hallinnan apuna käytetään mm. arkistonmuodostussuunnitelmaa ja tarvittavia rekistereitä ja luetteloja. Tietoaineistojen saatavuutta ja käytettävyyttä sekä eheyttä ja luottamuksellisuutta hallitaan luokittelemalla aineisto eri luokkiin tiedolle asetettujen vaatimusten pohjalta.

7.1 Luokittelun piiriin kuuluvat asiakirjat ja luokittelun perusteet

Tietoaineistojen käsittelyä ohjataan suojaustasojen (TTA 9 §) avulla. Luokittelun piiriin otetaan ensisijaisesti salassa pidettävät asiakirjat. Viranomaisen asiakirja on pidettävä salassa, jos se julkisuuslaissa tai muussa laissa on säädetty salassa pidettäväksi tai jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. Tuomioistuimet voivat myös lain nojalla määrätä asiakirjan salassa pidettäväksi.

Kaikkia salassa pidettäviä asiakirjoja ei ole tarpeen eikä tietoturvallisuusasetuksen mukaan mahdollistakaan luokitella suojaustasoihin. Luokittelu on mahdollista vain, jos tietoturvallisuusasetuksen 9 §:n 1 momentissa määritellyt vaikutukset voivat syntyä tiedon oikeudettomasta paljastamisesta. Se, että asiakirja on säädetty salassa pidettäväksi, ei vielä yksistään määritä sitä, mihin suojaustasoon asiakirja tulisi osoittaa kuuluvaksi. *Kukin tietoaineisto ja sen paljastumisesta aiheutuvat seuraukset on arvioitava konkreettisesti ja ottaen huomioon suojattava etu kokonaisuutena.*

Tietoturvallisuusasetuksen 9 §:n 2 momentissa on määritelty ne muut asiakirjat, jotka voidaan luokitella suojaustasoa IV edellyttäväksi asiakirjaksi. Tällaisia ovat sellaiset asiakirjat ja niihin sisältyvät tiedot, joiden luovuttaminen on viranomaisen harkinnassa (esim. harkinnanvaraisesti julkiset asiakirjat; julkisuuslaki 9 § 2 mom.) tai joita saadaan lain mukaan luovuttaa vain määrättyyn tarkoitukseen (esim. henkilörekisterit, julkisuuslaki 16 § 3 mom.).

Luokitusta ei saa ulottaa sellaisiin asiakirjoihin tai asiakirjan osiin, joissa käsittelyvaatimusten noudattaminen ei ole suojattavan edun vuoksi tarpeen. Luokittelu voidaankin tehdä siten, että tietoturvallisuutta koskevat vaatimuk-

set kohdistetaan vain sellaisiin asiakirjoihin tai asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen (tietoturvallisuusasetus 8 § 1 mom.).

Viranomainen ohjeistaa asiakirjojen luokittelun omassa toimintaympäristössään.

Asiakirjan allekirjoittaja tai työjärjestyksessä erikseen määrätty henkilö päättää luokitusmerkinnän tekemisestä asiakirjaan. Luokitus kertoo laatijan ja allekirjoittajan käsityksen siitä, millä tavalla asiakirja on suojattava.

On huomattava, ettei asiakirjan sisältämän salassa pidettävän tiedon paljastaminen sivullisille ole sallittua, vaikka asiakirjaan ei olisi merkitty suojaustasoa. Luokitusmerkintä saattaa puuttua esim. sellaisissa tapauksissa, joissa salassa pidettävä tieto käsittää laajassa asiakirjassa tai tietokokonaisuudessa vain pienen osan (esim. nimen tai luvun) tai kun esim. jokin asiakirjan liite on salassa pidettävä, vaikka asiakirja muutoin on julkinen. Luokitusmerkintä voi puuttua myös sen vuoksi, että salassa pidettävän asiakirjan paljastumisesta ei arvioida aiheutuvan tietoturvallisuusasetuksen 9 §:n 1 momentissa säädettyjä seurauksia.

Luokitusmerkintä ei vapauta tekemästä asiakirjasta julkisuuslain mukaista arviointia – luokitusmerkintä ei sellaisenaan synnytä salassapitovelvollisuutta suhteessa asiakirjaa lain mukaan pyytävään. Asiakirja voi olla salassa pidettävä vain julkisuuslain tai muun lain nojalla.

Sellaiseen salassa pidettävään asiakirjaan, jonka tietojen oikeudeton paljastuminen voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille julkisuuslain 24 §:n 1 momentin 2, 7 – 10 kohdissa tarkoitetulla tavalla, voidaan tehdä turvallisuusluokitusmerkintä (TTA 11 §).

Luokiteltavaan kansallisessa käytössä olevaan asiakirjaan tehdään vain suojaustasoa koskeva merkintä. Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin tietoturvallisuusasetuksen 11 §:n 1 momentissa säädetyissä tapauksissa, jollei kansainvälisistä tietoturvallisuusvelvoitteista muuta johdu tai asiakirja ei muutoin liity kansainväliseen toimintaan (11 § 3 momentti).

Koska ilmaisu ”LUOTTAMUKSELLINEN” on tietoturvallisuusasetuksessa tarkoitettu turvallisuusluokitusmerkintä, asiakirjaan ei ole lainmukaista tehdä tätä vastaavaa merkintää muulloin, kuin kysymyksen todella ollessa kyseiseen suojaustasoon kuuluvasta asiakirjasta.

7.2 Salassapitomerkinnät

Viranomaisen on tehtävä salassapitomerkintä asiakirjaan, jonka se antaa asianosaiselle ja joka on salassa pidettävä toisen tai yleisen edun vuoksi (JulkL 25 §). 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.

Tietojärjestelmien yhteydessä salassapitomerkinnät voidaan toteuttaa erilaisin menetelmin. Asianhallinnan metatietomäärityksen (SÄHKE2) mukaan salassapitoa koskevat metatiedot tulevat oletusarvoisina arkistonmuodostussuunnitelmasta. Tällöin salassapitomerkinnät ja niiden elinkaaret, kuten salassapidon päättyminen, voidaan kuvata metatieto-osuuksissa. Tieto salassapidon luonteesta ja tasosta tulee käydä ilmi käyttäjälle kuvaruudun näytöstä erilaisissa käsittelyvaiheissa. Käyttäjän tulee hallita riittävän hyvin käyttämänsä sovelluksen ominaisuudet, jotta pystyy tunnistamaan salassapitoa tai muita rajoituksia edellyttävän tiedon muusta tietovarannosta.

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).

Jos salassapito perustuu säännökseen, jossa on vahinkoedellytyslauseke (vähäinen vahinko, toimintaa vaarantava, loukkaa merkittävästi, vaarantaa keskeisiä tiettyjä etuja) merkintä voidaan tehdä kuitenkin niin, että siitä ilmenee vain se säännös, johon salassapito perustuu.

Vahingon edellytyslausekkeella tarkoitetaan salassapitosäännöstä, jossa salassapito on riippuvainen tiedon paljastumisesta asiattomalle taholle ja siitä aiheutuvista vahingoista organisaatiolle (esim. julkisuuslain 24 §:n 1 momentin 1, 2, 3 ja 6 – 15 kohdat). Katso tarkempia tietoja oikeusministeriön kotisivulta (www.om.fi, Perussäännökset, Julkisuuslaki, Oikeusministeriön 23.9.2005 ministeriöille julkisuuslainsäädännön täytäntöönpanosta ja osittaistarkistuksesta lähettämä kirje liitteineen).

Jos salassapito päättyy tiettynä hetkenä tai tietyn tapahtuman johdosta, tästä voidaan tehdä merkintä salassapitoa osoittavan leiman alapuolelle esim. käsin kirjaamalla sekä perusteluineen ellei tätä mahdollisuutta ole teknisessä ratkaisussa (metatieto) huomioitu etukäteen.

Tiedon salassa pitäminen lakkaa, kun asiakirjan antamisesta ei aiheudu salassapidon edellytyksenä olevia vaikutuksia tai kun julkisuuslain 31 §:ssä säädetty salassapitoaika on kulunut umpeen.

7.3 Suojaustasot ja niitä koskevat merkinnät

Viranomaisten luokiteltujen asiakirjojen käsittelyä ohjataan suojaustasojen (ST) avulla.

Suojaustasot ovat:

- suojaustaso I (ST I), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille
- suojaustaso II (ST II), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille
- suojaustaso III (ST III), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleisille tai yksityisille eduille ja oikeuksille
- suojaustaso IV (ST IV), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleisille tai yksityisille eduille tai, jos kysymys on tietoturvallisuusasetuksen 9 §:n 2 momentissa tarkoitetuista asiakirjoista, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Suosituksena on, että luokittelua käytetään vain salassa pidettäviin asiakirjoihin. Siten esim. henkilörekisteritiedot luokitellaan vain, jos henkilörekisterin tiedot ovat joko kokonaan tai joiltakin osin salassa pidettäviä tai jos henkilörekisteriin talletetaan henkilötietolain 11 §:ssä tarkoitettuja arkaluonteisia tietoja.

Pääsääntönä on, että salassa pidettävään asiakirjaan tehdään suojaustasoa koskeva merkintä (leima). Jos asiakirjaan voidaan tehdä turvallisuusluokitusmerkintä, sillä voidaan korvata suojaustasomerkintä (tietoturvallisuusasetus 11 § 1 mom.). Käytettävät merkinnät (leimat) on esitetty liitteessä 2.

Luokitusmerkintä voidaan jättää tekemättä, jos kaikki asiakirjaa käsittelevät ovat tietoisia asiakirjan salassapidosta ja sen käsittelyssä noudatettavista menettelytavoista. Esimerkiksi tietojärjestelmissä, joissa erikseen valtuutetut henkilöt käsittelevät pelkästään henkilörekisteriin kuuluvia henkilötietoja, ei edellytetä liitteessä 1 mainittujen merkintöjen käyttämistä normaaleissa käsittelytilanteissa. Tietoja käsittelevien tulee kuitenkin ehdottomasti tunnistaa näiden asiakirjojen ja tietojen käsittelyyn sisältyvät käyttörajoitukset.

Asiakirjaan tehtävää luokitusmerkintää ei suositella tehtäväksi myöskään silloin, kun salassapitovelvollisuus ja siitä johtuvat käsittelyvaatimukset ovat voimassa 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 (tietoturvallisuusasetus 10 § 2 mom.).

Suojaustaso tulee ilmaista käyttäjälle kyseessä olevaa luokkaa ilmaisevalla merkinnällä.

Viranomaisen asiakirjaa ei saa pitää salassa, kun salassapidolle laissa säädetty tai lain nojalla määrätty aika on kulunut. Tällöin poistuvat myös perusteet luokitukselle.

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.

Sellainen viranomaisen hallussa oleva asiakirja, johon sisältyviä tietoja saadaan käyttää vain tiettyyn tarkoitukseen, voidaan tietoturvallisuusasetuksen mukaisten edellytysten täyttyessä luokitella.

7.4 Tietoaineiston ryhmittely suojaustasoihin

Salassa pidettävä tietoaineisto sijoitetaan tiedon merkityksen ja sen paljastumisen seurausten mukaan määräytyvään suojaustasoon, jos tietoturvallisuusasetuksen 9 §:n 1 momentissa säädetyt edellytykset täyttyvät. Oikean luokan määritteleminen on tehtävä huolella. Suojaustasovaatimusta ei saa ulottaa sellaisiin tietoaineistojen osiin, joissa käsittelyvaatimusten noudattaminen ei suojattavan edun vuoksi ole tarpeen (Tietoturvallisuusasetus 8 § 1 mom.). On myös syytä huomata, että kaikkia salassa pidettäviä asiakirjoja ei välttämättä ole tarpeen eikä sallittuakaan luokitella.

Jo asiakirjaa laadittaessa tulee ottaa huomioon asiakirjan tai tiedon käsittelytarve. Asiakirjat tulee laatia siten, että niiden käsittely tukee tiedon saatavuutta, tiedon eheyttä sekä salassapidon ja käyttörajoitusten toteuttamista.

Asiakirjojen oletusarvoinen suojaustaso ja tarve käyttää turvallisuusluokitusmerkintää voidaan määritellä arkistonmuodostussuunnitelmissa. Kunkin asiakirjan luokitustarve ja luokka tulee kuitenkin aina arvioida erikseen sekä tehdä tätä vastaavien tietojen merkitsemisestä asiakirjaan tai sen metatietomäärittelyihin.

Yleisenä periaatteena on pitää julkinen ja salassa pidettävä tieto erillään. Tästä syystä asiakirjojen laadinnassa tulee kiinnittää huomio siihen, mikä osuus voidaan toteuttaa julkisen asiakirja-aineiston avulla ja mikä osuus edellyttää erillisenä käsiteltävissä olevan (hyvä julkisuus- ja salassapitorakenne) asiakirjan laadintaa.

Eri suojaustasoihin kuuluva tieto tulisi pääsääntöisesti sijoittaa eri asiakirjoihin, jolloin mahdollistetaan asiakirjojen käytettävyys ja hallinta elinkaaren aikana.

Asiakirjojen laadinnassa tulee ottaa huomioon asiakirjan sisältämän tiedon tarvitsijoiden laajuus. Asiakirjat, joissa jakelu kattaa laajan kohdejoukon, tulee kirjoittaa siten, että niitä voidaan käsitellä suojaustasolla ST IV tai ST III. Niissä voidaan viitata korkeamman suojaustason asiakirjoihin. Mitä aremmasta tiedosta on kysymys, sitä korkeampia turvajärjestelyjä edellytetään koko käsittelyketjulta.

Sellaiset viranomaisen asiakirjat, jotka vaativat ehkä laajaakin käsittelyä ja joiden paljastumisesta aiheutuva haitta tai luottamuksen menettäminen on vähäistä, luokitellaan suojaustasoon IV.

Edellä mainitut jakelun laajuuteen liittyvät rajoitukset liittyvät inhimillisen riskin hallintaan. Asiakirjat, joiden salassapitoaika on esimerkiksi 25 vuotta, edellyttävät hallittua tiedon käsittelyä koko salassapitoajan. Mitä laajemmalle joukolle tietoa jaetaan, sitä suurempi riski on salassapidon vaarantumiseen. On myös otettava huomioon, että suojaustasoihin I ja II kuuluvat asiakirjojen käsittely on oltava jäljitettävissä asiakirjan koko elinkaaren ajan (käsittelyloki, vast.).

Vaikka valmisteilla oleva asiakirja ei sisällä salassa pidettäviä tietoja, se voidaan luokitella suojaustasoon IV, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. Viranomaisen toimintaedellytysten ei yleensä voida katsoa vaarantuvan, kun kysymys on yleisesti merkittävistä valmisteluasioista, minkä vuoksi luokituksen käytölle on varsin suppeat rajat. Joka tapauksessa luokitus ei miltään osin saa vaikuttaa julkisuuslaissa viranomaiselle säädettyjen valmistelun julkisuutta koskevien velvoitteiden toteuttamiseen (JulkL 19 §).

Eräissä tapauksissa on syytä korostaa, mikä osuus asiakirjasta sisältää salassa pidettävää tietoa tai muuta luokiteltua tietoa. Tämä korostaminen voidaan toteuttaa esimerkiksi kappale- tai lukukohtaisesti. Luokiteltua tietoa sisältävän kappaleen alkuun voidaan merkitä sulkuihin suojaustasoa osoittavan luokkaa koskeva merkintä osoittamaan kappaleeseen sisältyvän informaation käsittelyn tasoa. Tämä merkintätapa auttaa myöhemmin asiakirjojen käsittelijöitä tunnistamaan erityiskäsittelyä edellyttävät osuudet asiakirjassa ja arvioimaan tarpeen luokittelun jatkumiselle. Tämä helpottaa myös niissä tilanteissa, joissa uusien asiakirjojen laadinnassa käytetään apuna olemassa olevaa tietovarantoa.

Luokiteltu aineisto on merkittävä suojaustasojen avulla, kun sitä luovutetaan edelleen. Samalla on varmistuttava, että luovutus on lain mukaan mahdollinen ja että vastaanottaja täyttää tietoaineiston käsittelyltä vaadittavat edellytykset. Luokiteltava aineisto suositellaan merkittäväksi liitteessä 2 mainituilla leimoilla ja merkinnöillä aina koko asiakirjan elinkaaren ajan aina siihen asti, kun se on salassa pidettävä.

7.5 Turvallisuusluokitusmerkinnät

Viranomaisten asiakirjoihin voidaan tehdä turvallisuusluokitusmerkintä tietoturvallisuusasetuksen 12 §:ssä osoitetuissa tapauksissa. Turvallisuusluokitusmerkintöjä on neljää eri tasoa osoittavaa. Turvallisuusluokiteltua aineistoa käsitellään kohdassa 7.3 mainituille vastaaville suojaustasoille annettujen vaatimusten mukaisesti.

Turvallisuusluokitusmerkinnät ovat:

- suojaustaso I: ERITTÄIN SALAINEN, jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille
- suojaustaso II: SALAINEN, jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille
- suojaustaso III: LUOTTAMUKSELLINEN, jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille
- suojaustaso IV: KÄYTTÖ RAJOITETTU, jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa julkisuuslain 24 § 1 mom. 2,7 – 10 kohdassa tarkoitetuille yleisille eduille.

Huom! Turvallisuusluokiteltavien asiakirjojen yhteydessä käytetään usein ilmaisua turvallisuusluokka. Viranomainen voi omassa toiminnassaan käyttää sopivia organisaatiokohtaisia ilmaisuja ja lyhenteitä. Myös kansainvälisessä turvallisuusluokitellun tietoaineiston yhteydessä käytetään ilmaisuja turvallisuusluokka I – IV, joihin kuuluvaa aineistoa suojataan tässä ohjeessa mainittujen suojaustasojen I – IV mukaisesti.

Turvallisuusluokitusmerkintöjä koskevat leimat on esitetty liitteessä 2.

Suojaustasojen ja turvallisuusluokittelunimikkeiden vastaavuus on esitetty oheisessa taulukossa.

Suojaustaso	Turvallisuusluokittelun nimike	Lyhenne
Suojaustaso I	ERITTÄIN SALAINEN	ERSAL (E)
Suojaustaso II	SALAINEN	SAL (S)
Suojaustaso III	LUOTTAMUKSELLINEN	LUOT (L)
Suojaustaso IV	KÄYTTÖ RAJOITETTU	RAJ (R)

Lyhenteitä voidaan käyttää tietojärjestelmissä ja asiakirjoissa soveltuvin osin.

Ilmaistaessa kunkin suojaustason mukainen turvallisuusluokitus kappalekohtaisesti, merkitään kappaleen alkuun esim. sulkuja käyttäen kyseinen luokitusmerkintä. Esimerkiksi (S) kappaleen alussa viittaa kyseisen kappaleen sisältävän SALAINEN luokan tietoa. Vastaavasti metatietojen yhteydessä suositellaan käytettäväksi pidempää lyhennettä, kuten SAL. Jos tietojärjestelmän ominaisuudet asettavat rajoituksia lyhenteen pituudelle, voidaan käyttää lyhyempiä muotoja kuten esimerkiksi ERS ja LUO lyhenteiden ERSAL ja LUOT sijasta.

Suojaustasoihin I – III kuuluva tieto tulee esittää käyttäjälle sähköisissä näytöissä ko luokkaa ilmaisevalla merkinnällä.

Turvallisuusluokitusmerkinnällä ERITTÄIN SALAINEN merkittyjen asiakirjojen jakelu tulisi tarkkaan harkita tarveperustaisesti, ja huomioiden salassapitoaikavaatimus (käsittelyoikeus). Muutoinkin I suojaustasoon kuuluvan asiakirjan jakelusta päättää aina laatija ja allekirjoittaja. Turvallisuusluokitusmerkinnällä ERITTÄIN SALAINEN varustetusta asiakirjasta ei saa ottaa kopioita, eikä jakaa eteenpäin ilman asiakirjan laatijan tai allekirjoittajan kirjallista lupaa.

Asiakirjojen, joissa käytetään turvallisuusluokitusmerkintää SALAINEN, jakelu tulisi rajoittaa tarveperustaisesti huomioiden salassapitoaikavaatimus.

7.6 Kansainvälisten aineistojen turvallisuusluokittelu

Kansainvälisiltä järjestöiltä ja toisilta valtioilta tulleissa asiakirjoissa voi olla järjestöjen ja valtioiden omia luokitusmerkintöjä. Niihin tehdään Suomen vastaavaa turvallisuusluokitusta 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 turvallisuusluokiteltu 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 (JulkL 24.1 § 2,7,-10 k).

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

Kohde	SUOJAUSTASO I	SUOJAUSTASO II	SUOJAUSTASO III	SUOJAUSTASO IV
Suomi	ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITETTU
EU	TRÉS SECRET UE/ EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED

EU:n sisäiset asiakirjat, jotka on merkitty "LIMITE" merkinnällä, tarkoittavat näiden jakelun rajoittamista. Kyseessä ei ole turvallisuusluokitusta 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.

7.7 Henkilötietojen luokitus ja merkinnät

Henkilötietojen käsittelyä ja henkilörekistereitä ohjaavat henkilötietolaki, julkisuuslaki 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.

Mikäli asiakirjan muusta sisällöstä ei muuta johdu, henkilötietoja sisältävien asiakirjojen suojaustaso voi olla joko ST III tai ST IV tietoturvallisuusasetuksen 9 §:n 1 momentin perusteella tehdyn vaikutusarvioinnin mukaan.

Vaikka yksityisyyden suojan vuoksi tiettyjä asiakirjoja koskisikin ehdoton salassapitovelvoite, kaikki salassa pidettävät henkilöä koskevat asiakirjat tai niiden tiedot eivät välttämättä kuulu suojaustasoon III. Salassapidon perusteena yksityisyyden suojaa koskevia salassapitosäännöksiä säädettäessä on ollut yleisellä tasolla tehty arvio tietojen julkisuudesta johtuvasta yksityisyyden suojan vaarantumisen riskistä (HE 30/1998 vp., s. 88). Suojaustasojen mukaisessa luokittelussa sen sijaan on kysymys sen arvioimisesta, mitkä salassapitovelvollisuuden piiriin kuuluvista tiedoista ovat sellaisia, että ne konkreettisesti voivat vahingoittaa yksityisyyden suojaa oikeusjärjestyksen suojaamana oikeushyvänä.

Henkilötietoja ei tarvitse erikseen merkitä leimojen avulla, jos niitä käsittelevät vain riittävän koulutuksen saaneet, käyttövaltuudet omaavat henkilöt.

Henkilötietojen käsittelyssä on toteutettava tarpeellisuus- ja virheettömyysvaatimukset sekä suojaamis- ja huolellisuusvelvoitteet. Tätä varten on oltava toimiva käyttövaltuus-hallinta sekä seuranta- ja valvontajärjestelmä.

Arkaluonteisten tai biometristen henkilörekisteriin talletettujen henkilötietojen käsittelytapahtumien tulee kirjautua lokiin (TTA 20 § 1 mom.).

Henkilötunnuksen käytössä on otettava huomioon HetiL 9 § ja HetiL 13 §:t. Henkilötunnuksen sisältäviä asiakirjoja on käsiteltävä suojaustason IV mukaisesti, ellei asiakirjan sisällön perusteella asiakirjaa kuulu käsitellä korkeamman suojaustason vaatimusten mukaisesti.

7.8 Laajojen tietovarantojen luokittelua koskevat suositukset

Laajoilla tietovarannoilla tarkoitetaan tässä yhteydessä yhteen tai useampaan paikkaan talletettuja tietoaineistoja, joihin käyttäjä pääsee kerralla käsiksi. Tieto on kerätty useista eri lähteistä ja tietoja yhdistelemällä muodostetaan uutta tietoa eri käyttötarkoituksiin.

Vaikka tietovarantoon sisältyvät yksittäiset asiakirjat olisivat julkisia tai alhaiseen suojaustasoon luokiteltavia, saattaa tietovaranto muodostaa kokonaisuuden, jonka suojaustarve on siihen sisältyviä yksittäisiä asiakirjoja korkeampi. Esimerkiksi tiedon paljastuminen henkilön omistamista aseista saattaa aiheuttaa haittaa yksityiselle edulle, mutta koko maan aserekisterin tiedot voivat aiheuttaa vahinkoa yleiselle turvallisuudelle.

Kunkin tietovarannon suojaustasovaatimus määräytyy sen sisältämien yksittäisten asiakirjojen suojaustasovaatimusten pohjalta. Tietoturvallisuusasetus säätää vähimmäistason luokiteltavien asiakirjojen tietoturvavaatimukselle. Asetus ei sen 7 §:n 2 momentin mukaan estä viranomaista soveltamasta omassa toiminnassaan tietoturvallisuusasetuksen luvussa 4 säädettyä korkeampia tietoturvavaatimuksia. Onkin suositeltavaa, että viranomainen arvioi koko tietovarannon suojaustarpeen sekä käyttää tarvittaessa yksittäisten asiakirjojen arviointia laajempaa vaikutusarviointia tietovarannon suojaustarpeesta ja soveltaa sen mukaisia tietoturvamenettelyitä.

Tarjottaessa käyttöoikeuksia erilaisiin tietovarantoihin, tulee aina kiinnittää erityistä huomiota käyttöoikeuksien määrittelyyn ja niiden valvontaan.

Kunkin tietojärjestelmän toteutuksessa ja toimintojen määrittelyssä tulee ottaa huomioon, minkä suojaustason mukaisilla järjestelyillä kyseisiä asiakirjoja ja tietovarantoja voidaan käsitellä.

Laajoja tietovarantoja käsittelevät yleensä tietojenkäsittelyn ammattilaiset tai tehtyjen sopimusten nojalla tietojenkäsittelyä tai turvapalveluja tarjoavat yritykset. On tärkeää, että päätökset suojaustasoista ja noudatettavista menettelyistä sekä turvatoimien järjestelyistä tekevät eri henkilöt kuin tietovarantoja käsittelevät henkilöt.

Tietovarantojen käyttöoikeuksien määrittelyssä tulee varmistaa, ettei synny tilanteita, joissa käyttöoikeuden haltija pääsee käsiksi hänelle kuulumattomiin tietoihin.

Tietojärjestelmien ja toimintojen toteutuksessa tulee ottaa huomioon kaikki tiedon käsittelyvaiheet siten, että ne voidaan suorittaa riittävän suojaustason tarjoavassa ympäristössä.

Kaikissa tietovarannoissa voidaan käyttää käyttöoikeuden tarkistamismenettelyä riippumatta siitä, sisältääkö kyseinen tietovaranto salassa pidettävää tietoa tai ei. Julkinen ja salassa pidettävä tieto on pidettävä erillään teknisin (verkko, levytila, salaus, käyttäjän tunnistus) ja hallinnollisin keinoin (käyttöoikeudet, lokit, tunnistus). Tietojärjestelmien suunnittelussa ja käyttöoikeuk-

sien hallinnassa tulee kiinnittää huomiota siihen, että viranomaisessa tietotyötä tekevät saavat käyttöönsä työtehtäviensä edellyttämät tiedot.

7.9 Tiedon eheydelle ja kiistämättömyydelle asetettavia vaatimuksia

Viranomaisten asiakirjoille ja niihin sisältyville tiedoille asetetaan tiedon merkityksen ja käytön vuoksi erilaisia tiedon eheyttä ja kiistämättömyyttä koskevia vaatimuksia. Tällaisia vaatimuksia sisältyy esimerkiksi kaikkeen rahaliikenteeseen ja niihin asiakirjoihin, joilta edellytetään viranomaisen allekirjoitusta. Näissä tilanteissa viranomaisen tulee varmistaa menettelyt, että annetut tiedot ovat muuttumattomia ja oikeita ja että alkuperäiset asiakirjat ovat todennettavissa.

Asiakirjan sähköisessä tallettamisessa ja siirtämisessä on käytettävissä erilaiset tiivistefunktiot ja sähköiset allekirjoitukset eheyden ja kiistämättömyyden varmistamiseksi.

Sähköisessä tiedonsiirrossa tulee toimivaltaisen viranomaisen toimenpitein varmistaa, että viranomaisen välittämät ja ylläpitämät tiedot siirretään niin turvallisesti, etteivät ulkopuoliset pääse niitä tahattomasti muuttamaan.

Viranomainen voi luokitella tietoaineistojaan eheysvaatimusten pohjalta. Esimerkiksi (1) virheettömyyttä edellyttävä tieto ja (2) muut tiedot.

7.10 Tiedon saatavuudelle ja käytettävyydelle asetettavia vaatimuksia

Viranomaisen tiedon käytettävyysvaatimukset riippuvat tiedon sisällöstä ja sen käyttötarpeista. Monet toimintaprosessit asettavat suuria vaatimuksia oikea-aikaisen ja oikean tiedon saatavuudelle. Julkisuuslaissa määritellään vaatimukset tiedon antamisesta sitä pyytävälle. Tiedon käytettävyysvaatimus nousee esille myös hyvän tiedonhallintatavan toteuttamistarpeesta. Käytettävyyteen sisältyy useita elementtejä. Käytettävyys riippuu esim. tietoverkon ominaisuuksista, varmentamisista, tietojärjestelmän käyttöliitynnän toteutuksesta, työaseman ominaisuuksista ja käyttäjän osaamisesta.

Eri asiakirjoilla on yleensä erilainen käyttötarve toiminnan kannalta. Jos toimintaprosessissa käsitellään korkeaa suojaustasoa ja korkeaa käytettävyyttä sisältäviä tietoja tai asiakirjoja, korostuvat tiedon käsittelyyn sisältyvät vaatimukset. Nämä vaatimukset on otettava huomioon tietojärjestelmien suunnittelusta alkaen. Tällaista tietoa sisältyy usein erilaisiin valvontajärjestelmien tuottamaan ja käsittelemään tietoon.

Julkisten asiakirjojen ja tietojen käsittelyssä on tarpeen kiinnittää erityistä huomiota tiedon käytettävyyden ja asiasta riippuen myös tiedon eheydelle ase-

tettujen vaatimusten toteutumiseen. Käytettävyyden kannalta tämä tarkoittaa mm. sitä, että kyseiset tiedot ovat niitä työtehtävissään tarvitsevien käytettävissä mahdollisimman helposti, jopa siinä laajuudessa, että ne työtehtävien edellyttämällä tavalla ovat kiinteä osa työprosessia.

Tiedon kriittisyydellä tarkoitetaan niitä vaatimuksia, joita toiminnan toteuttaminen edellyttää. Kun jokin toiminta edellyttää tietyn tietovarannon välitöntä saatavuutta, on kysymys kriittisestä tiedosta. Esimerkkejä kriittisestä tiedosta:

- projektikokous (tieto paikasta ja ajankohdasta sekä osallistumistarpeesta)
- koulutustilaisuus (tieto kouluttajista, koulutustavoitteista ja opetusmateriaalista).

Tiedon saatavuutta voidaan tarkastella esim. prosessin näkökulmasta:

- toiminnan toteuttamisen kannalta erittäin tärkeät asiakirjat ja tiedot
- toiminnan toteuttamisen kannalta tärkeät asiakirjat ja tiedot
- toimintaa tukevat asiakirjat
- muut asiakirjat.

Usein toiminta edellyttää sekä julkista että salassa pidettävää tietoa. Toiminnasta vastaavan tulee tunnistaa toiminnan edellyttämä tieto. Suunniteltaessa ja kehitettäessä tietotyön edellyttämiä rakenteita tulee kiinnittää erityistä huomiota siihen, että toimintojen tarvitseman kriittisen tiedon saatavuus on turvattu ja varmennettu. Viranomaisen tulee etukäteen tunnistaa ja määrittää toiminnan edellyttämä kriittinen tieto.

8 Luokiteltujen tietoaineistojen käsittelyvaatimuksia

Ohjeistuksen tavoitteena on luoda yhtenäiset menettelyt ja edellytykset tietoaineistojen käsittelyyn valtionhallinnossa. Samalla pyritään yhdenmukaistamaan menettelyt kansallisten ja kansainvälisten luokiteltujen asiakirjojen osalta elinkaaren erilaisissa käsittelytilanteissa.

Kansainvälisten velvoitteiden vaatimukset eroavat tietoturvallisuusasetuksessa ja näissä ohjeissa osoitetuista toimenpiteistä jonkin verran, mistä syystä kansainvälisten velvoitteiden alaisessa toiminnassa on tutustuttava velvoitteisiin tapauskohtaisesti.

8.1 Perusvaatimuksia

Tietoaineistojen käsittelylle asetettavat vaatimukset koskevat koko tiedon elinkaarta. Erityisesti tiedon salassapitoajalle asetetaan useita kriittisiä vaatimuksia. Tiedon käsittelijä on erityisessä asemassa näiden vaatimusten toteuttamisessa. Hän vastaa kaikissa tietotyön tilanteissa siitä, että henkilökohtainen tiedon käsittely tapahtuu oikein ja työnantajan hänelle antamilla työvälineillä.

Viranomaisen tiedolle on ominaista, että tiedolle on tunnistettava tai määriteltävä toimivaltaa käyttävä viranomainen tai hänen edustajansa. Tällä toimivaltaa käyttävällä viranomaisella on keskeinen vastuu hänen toimivaltaansa kuuluvasta tiedosta. Viranomaisen tulisi määritellä kaikille tietoaineistoilleen ja järjestelmilleen vastuutahot. Merkintöjä (kuten leimat) voidaan toteuttaa valmiiksi esim. sähköisiin asiakirja- ja lomakepohjiin. Suojaustaso tulee tiedostaa koko tietoaineiston elinkaaren ajan.

Salassa pidettävän sähköisen asiakirjan käsittelyn tulee kirjautua sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai itse asiakirjaan. Sähköisen käsittelyn suositeltava kirjaamispaikka on loki tai vastaava sähköinen apuväline.

Suojaustason mukaista luokitusta edellyttävä tieto tulee tallentaa kyseiselle luokalle asetettujen vaatimusten mukaisesti. Käyttöoikeuden tarkistavissa ja toimivan, asiakirjakohtaisen käyttövaltuushallinnan sisältävissä valvotuissa korotetun tietoturvallisuustason verkoissa voidaan suojaustason III tieto tallettaa selväkielisenä.

Salassa pidettävät asiakirjat eivät ole julkisia vaan salassapitoperusteen mukaisesti salassa pidettäviä. Tämä tarkoittaa, että asiakirjan käsittelyyn ovat oikeutettuja ko. asiakirjassa tai asiaryhmässä mainitut tahot. Asiakirjasta saa antaa tietoja vain niille henkilöille, joille on myönnetty oikeus käsitellä asiakirjan edellyttämän suojaustason mukaisia asiakirjoja ja joilla on asiakirjan sisältämää tietoa edellyttävä, työtehtäviin pohjautuva käsittelytarve.

Oheisessa taulukossa on esitetty suojaustasoittain asiakirjojen ominaisuuksia käsittelyoikeuden, jakelun, jäljitettävyyden ja tietoteknisen käsittelyn osalta. Turvallisuusluokittelua edellyttävä aineisto käsitellään vastaavan suojaustason mukaisesti.

	ST IV	ST III	ST II	ST I
Käsittelyoikeus	Myönnetty käsittelyoikeus	Myönnetty käsittelyoikeus	Myönnetty käsittelyoikeus	Jakelussa mainittu, myönnetty käsittelyoikeus
Jakelu	Työtehtävien mukaisesti	Työtehtävien mukaisesti	Laatija määrittelee, perustuu työtehtäviin	Laatija määrittelee henkilöjakelun
Käsittelyn kirjaaminen	Henkilörekisterissä olevien tietojen tai biometristä tietoa sisältävien asiakirjojen käsittelytapahtumien kirjaaminen	Arkaluonteisten henkilörekisterissä olevien tietojen tai biometristä tietoa sisältävien asiakirjojen käsittelytapahtumien kirjaaminen.		
Muiden osalta suositellaan	Käsittelytapahtumien kirjaaminen	Käsittelytapahtumien kirjaaminen		
Jäljitettävyys	Ei seurantaa	Ei seurantaa	Asiakirjakopiokohtainen jäljitettävyys	Asiakirjakopiokohtainen jäljitettävyys
Siirto avoimissa verkoissa	Salattuna tai muutoin suojattuna	Salattuna tai muutoin suojattuna	Ei sallittu	Ei sallittu
Siirto viranomaisen verkoissa	Selväkielisenä perus- ja sitä korkeamman tietoturvallisuustason verkoissa	Selväkielisenä korotetun tai korkean tietoturvallisuustason verkoissa	Selväkielisenä valvotuissa korkean tietoturvallisuustason verkoissa	Vahvasti salattuna tai muutoin vahvasti suojattuna valvotuissa erillisverkoissa
Käsittely avoimeen verkkoon liitetyssä työasemassa	Sallittu perus-, ja sitä korkeamman tietoturvallisuustason käsittely-ympäristöissä	Sallittu korotetun tai korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu valvotuissa korkean tietoturvallisuustason käsittely-ympäristöissä	Ei sallittu
Käsittely viranomaisen verkkoon liitetyssä työasemassa	Sallittu perus- ja sitä korkeamman tietoturvallisuustason käsittely-ympäristöissä	Sallittu korotetun tai korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu valvotuissa korkean tietoturvallisuustason käsittely-ympäristöissä	Sallittu korkean tietoturvallisuustason erillisverkossa, johon ei ole yhteyttä muista tietoverkoista.
Tallentaminen muistivälineelle (kiintolevy, siirrettävä muisti)	Suojattuna	Salattuna tai muutoin suojattuna	Vahvasti salattuna tai muutoin vahvasti suojattuna	Vahvasti salattuna tai muutoin vahvasti suojattuna
Tallentaminen viranomaisen verkon palvelimelle	Suojattuna käyttäjätunnuksilla	Salattuna tai muutoin suojattuna korotetun tietoturvallisuustason käsittely-ympäristössä	Salattuna tai muutoin uojattuna, korkean tietoturvallisuustason käsittely-ympäristössä	Vahvasti salattuna tai muutoin vahvasti suojattuna, jos järjestelmä täyttää korkean tietoturvallisuustason vaatimukset.

Tarkemmat käsittelyohjeet suojaustasoittain on esitetty liitteessä 4.

Asiakirjojen käsittelyä ohjaava luokitus (suojaustaso ST) ilmaistaan tähän tarkoitukseen osoitetulla merkinnällä (liite 2). Merkinnän tekee joko aineiston laatija, ensimmäinen vastaanottaja tai se, jolla on oikeus päättää kyseisen aineiston käsittelystä ja käytöstä. Luokitusmerkinnästä päättää asiakirjan allekirjoittaja joko manuaalisella tai sähköisellä allekirjoituksellaan.

Asiakirjojen luokitusta vastaavat käsittelyvaatimukset riippuvat asiakirjojen sisältämien tietojen paljastumisen aiheuttaman vahingon merkittävyydestä salassapitosäännösten suojaamille yleisille tai yksityisille eduille.

Salassa pidettävien viranomaisten asiakirjojen salassapitoaika ei ole riippuvainen siitä, onko asiakirja luokiteltu tai onko siihen tehty merkintää salassapidosta. Kaikki luokitellut asiakirjat ovat salassa pidettäviä niin kauan kuin salassapidon peruste on olemassa, kuitenkin enintään 25 vuotta asiakirjan allekirjoittamisesta. Eräissä erikoistapauksissa salassapitoaika voi olla pidempi.

Salassa pidettävästä asiakirjasta voi luovuttaa tiedon sivulliselle vain, jos tiedon antamisesta tai oikeudesta tiedon saamiseen on lailla erikseen nimenomaisesti säädetty.

Niissä toimeksiannoissa tai yhteistoimintahankkeissa (vast.), joissa ulkopuolisten tahojen kanssa on tarve käsitellä viranomaisen salassa pidettävää tietoa, tulee täyttää etukäteen seuraavat edellytykset:

- ulkomaisen tahon turvallisuus on varmistettu laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) kuvatun menettelyn mukaisesti
- tiedon luovuttamisessa noudatetaan tämän ohjeen mukaisia menettelyjä
- asianomaisella organisaatiolla on kyseisen suojaustason edellyttämät tiedon käsittelyn vaatimat toimitilat ja menettelyt
- tietoon oikeutetut henkilöt tuntevat viranomaisen käsittelysäännöt salassa pidettävien asiakirjojen ja tietojen osalta.

Toimeksiantoon tulee tarvittaessa sisällyttää turvallisuusjärjestelyjä koskeva sopimus (esim. hankintasopimuksen liitteeksi). Mikäli ulkopuolisen tahon kanssa on sovittu laajasta, korkeaa suojaustasoa sisältävästä hankkeesta tai kumppanuudesta, on edellä mainitun lisäksi hyvä noudattaa alla mainittuja periaatteita:

- asianomaisen organisaation ja viranomaisen kesken laaditaan erillinen turvallisuussopimus, jossa määritetään toimeksiannoissa noudatettavat turvallisuusmenettelyt. Hankintojen kohdalla voidaan tarkentaa turvallisuusvaatimuksia hankinnan edellyttämien turvallisuusjärjestelyjen puitteissa.
- asianomaisen organisaation henkilöstöltä voidaan edellyttää erillisen viranomaisen määrittelemän vaitiolositoumuksen allekirjoittamista. Tämän tavoitteena on varmistaa henkilöiden tuntevan asetetut turvallisuusvelvoitteet.

Viranomaisen ulkopuolelle annetuista salassa pidettävistä asiakirjoista tulee tehdä asianomaiset kirjaukset.

Salassa pidettävää asiakirjaa tulee hallita asiakirjan sisältämien tietojen edellyttämän suojaustason asettamien vaatimusten mukaisesti asiakirjan koko elinkaaren ajan, valmistelusta tuhoamiseen asti.

Tietojärjestelmätoteutuksissa tulee ottaa huomioon niissä käsiteltävän tiedon edellyttämät suojaustasot. Työskentely-ympäristöt tulee suojata riittävin tilaturvallisuustoimenpitein siten, että ne ovat riittävästi valvottuja ja tarjoavat pääsyn vain tietoon oikeutetuille.

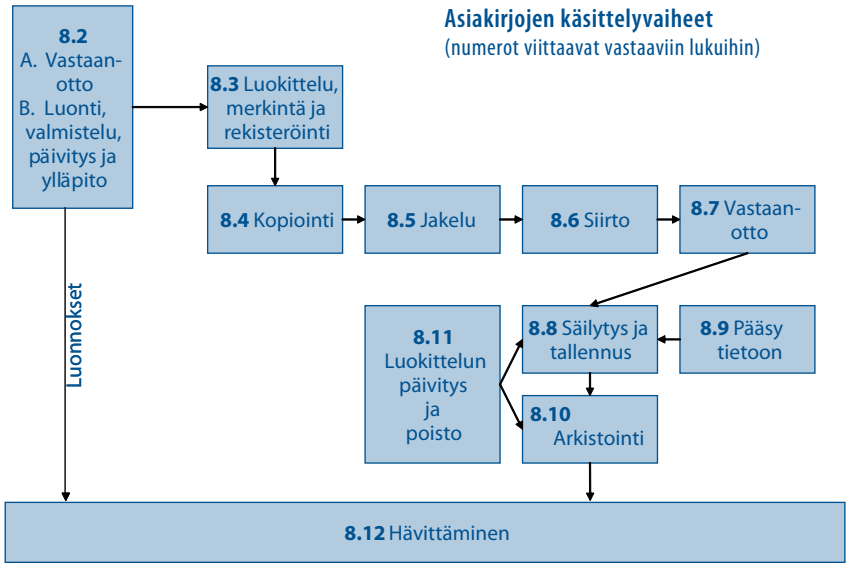
Mikäli asiakirjassa on sekä julkista että salassa pidettävää tietoa, tulee asiakirjasta käydä ilmi julkinen ja salassa pidettävä osuus.

Mikäli tietojärjestelmässä on sekä julkista että salassa pidettävää tietoa, suositellaan salassa pidettävien tietojen osalta suojaustason merkintää. Esimerkiksi tietokantapohjaisissa järjestelmissä asia voidaan määritellä taulu-, kenttä- tai tietokohtaisesti rakenteesta ja tietoaineistosta riippuen.

Asiakirja luokitellaan asiakirjan sisältämän tiedon edellyttämään suojaustasoa osoittavaan luokkaan. Jos asiakirja koostuu useista osista, esim. pääasiakirjasta ja liitteistä, varustetaan pääasiakirja sillä leimalla, mikä edustaa koko asiakirjan korkeinta luottamuksellisuustasoa. Tällöin pääasiakirjasta tulee käydä ilmi sekä pääasiakirjan että liitekohtainen suojaustaso, mikäli nämä poikkeavat toisistaan. Jos asiakirjaa ja sen liitteitä voidaan käsittelyn osalta pitää erillisinä asiakirjoina, voidaan myös niiden suojaustaso ilmoittaa kunkin osa-asiakirjan edellyttämällä tavalla.

Kun asiakirjassa on usean eri salassapitoperusteen mukaan salassa pidettävää tietoa, tulee asiakirjasta käydä ilmi nämä salassapidon perusteet. Tämä tieto korostuu mm. arvioitaessa asiakirjan jakelua ja tiedon antamista asiakirjan julkisesta ja salassa pidettävästä osuudesta sekä tarkasteltaessa asiakirjan salassapitoajan päättymistä.

Oheisessa kaaviossa on esitetty tyypillisen asiakirjan elinkaaren vaiheet.



8.2 Tietoaineistojen luonti ja editointi

Tietoaineistojen valmistelutyössä tulee alusta alkaen kiinnittää huomio siihen, onko kysymyksessä julkinen vai salassa pidettävää tietoa sisältävä aineisto. Valmistelussa oleva aineisto on laatijan ja valmisteluun osallistuvien vastuulla. Valmistelijataho päättää valmistelussa olevan asiakirjan jakelusta. Valmistelussa oleva asia ei pääsääntöisesti ole ulkopuolisille tarkoitettua, olipa kyseessä julkista tai salassa pidettävää tietoa sisältävä asiakirjaluonnos. Kun asiakirja saavuttaa tason, jossa siitä syntyy viranomaisen asiakirja, se otetaan osaksi viranomaisen tietovarantoa.

Luokiteltua tietoa sisältävää asiakirjaa on käsiteltävä sen valmistelun aikana samalla tavalla kuin viranomaisen muitakin asiakirjoja. Tiedon käsittely ei riipu siitä, missä muodossa tieto on talletettu.

Kun luokiteltua tietoa käsitellään dokumentoidussa muodossa, esim. tekstinä, kuvina, ääni- tai videonäytteinä, sähköisessä muodossa tietojärjestelmissä tai erilaisina tallenteina, tulee aina noudattaa niitä vaatimuksia, mitä viranomaisen asiakirjoista on edellytetty.

Kaikissa koulutuksissa, kokouksissa ja muissa esittelytilanteissa käytettävät tietoaineistot tulee valmistella siten, että niistä käy ilmi tiedon suojaustaso ja yksilöintitiedot (esim. päiväys, laatija ja dokumentin yksilöintitieto). Esittelymateriaalia on käsiteltävä kuten muitakin viranomaisen asiakirjoja tässä ohjeessa annettuja vaatimuksia noudattaen. Tällaista tietoaineistoa ovat mm. diarioimattomat ja kirjaamattomat esityskalvot.

Mikäli edellä mainituissa tilanteissa on välttämätöntä käsitellä suojaustasoon II (SALAINEN) tai I (ERITTÄIN SALAINEN) kuuluvaa aineistoa, tulee tästä käsittelystä jäädä asiakirjan käsittelyhistoriaan käsittelyyn osallistuneiden tiedot. Lisäksi on etukäteen varmistuttava siitä, että osanottajilla on kyseisen suojaustason edellyttämä käsittelyoikeus ja tarve esitettävään tietoon.

On erittäin suositeltavaa, ettei ylimpiin suojaustasoihin kuuluvaa tietoa esitetä tai talleteta viranomaisen asiakirja-aineiston ulkopuolella.

Asiakirjoissa voidaan viitata ylemmän suojaustason sisältämään asiakirjaan. Tämä koskee myös julkisia asiakirjoja.

Laadittaessa toimenpiteitä edellyttäviä asiakirjoja, tulee asia esittää siten, että kyseinen asiakirja voidaan luokitella mahdollisimman alas. Tällä menettelyllä saavutetaan toiminnan edellyttämä käytettävyys. Korkeampaa suojaustasoa edellyttävä täsmätieto (vast.) ilmaistaan vastaavasti perusasiakirjan viitetietoina.

Rakenteellisessa dokumentaatiossa ja metatiedoissa tulee ottaa huomioon samat viranomaisen asiakirjalle asetetut käsittelysäännöt. Käytettäessä asianhallintajärjestelmiä, joissa asiakirjoja hallitaan metatietoja sisältävien asiakirjojen avulla, tulee tavoitteena olla metatietoja sisältävän tietovarannon toteuttaminen siten, että siinä oleva tieto on mahdollisimman laajalti julkista tietovarantoa tai mahdollisimman matalaan suojaustasoon luokiteltua tietoa. Näillä toimenpiteillä edesautetaan hyvän tiedonhallintatavan toteuttamista.

Asiakirjojen laadinnassa tulee ottaa huomioon asiakirjan käyttötarkoitus sekä pyrkiä hyvään julkisuus- ja salassapitorakenteeseen, mikä merkitsee vaatimusta eriyttää mahdollisuuksien mukaan salassa pidettävät tiedot julkisesta tiedosta. Myös eri suojaustasoihin kuuluva tieto tulee ensisijaisesti esittää eri asiakirjoissa. Näillä menettelyillä turvataan asiakirjojen käytettävyysvaatimukset.

8.3 Aineistojen luokittelu, merkintä ja rekisteröinti

Asiakirjan laatija (yleensä asian esittelijä) tekee ehdotuksen asiakirjan luokittelusta. Luokittelusta päättää henkilö, joka muutoinkin päättää asiasta (esittelyasioissa ensimmäinen allekirjoittaja).

Asiakirja merkitään siihen sisältävien tietojen ylintä suojaustasoa vastaavalla merkinnällä. Jos suojaustasovaatimus kohdistuu vain osaan asiakirjaan, merkintä tehdään siten, että siitä ilmenee se asiakirjan osa, mihin suojaustasovaatimus kohdistuu.

Viranomaisen asiakirjarekisteristä tulisi käydä ilmi, mitä suojaustasoa asiakirjat edellyttävät. Korkeimman suojaustason edellyttämien asiakirjojen rekisteri voidaan tarvittaessa luokitella ja se tulee käyttöoikeuksin rajata asiakirjarekisterin muista tiedoista.

8.4 Kopiointi

Luokitelluista asiakirjoista voidaan myös ottaa sekä sähköisiä että paperimuotoisia kopioita ottamalla huomioon suojaustasokohtaiset rajoitukset ja käsittelysäännöt.

Kopioita tulee käsitellä kuten alkuperäisiä asiakirjoja.

Kopiot on merkittävä kuten alkuperäiset asiakirjat sekä varmistuttava, että kopion saajalla on työtehtäviin perustuva oikeus salassa pidettävän tietoaineiston käsittelyyn.

8.5 Asiakirjan jakelu

Asiakirjojen jakelu toteutetaan asiakirjan asettamien vaatimusten mukaisesti. Asiakirjan allekirjoittaja määrää jakelun ja käsittelyprosessin.

Asiakirjan luovuttamisen edellytyksenä on, että vastaanottajalla on aineiston hallintaan tarvittavat oikeudet.

Tietojärjestelmissä tietojen jakelu toteutetaan ensisijaisesti tarjoamalla pääsyoikeus tietoon tai sähköpostin välityksellä. Salassa pidettävän tiedon käsittelyn tulee tapahtua käyttöoikeuksien puitteissa ottaen huomioon suojaustasokohtaiset vaatimukset.

Jakelun laajentamisessa on otettava huomioon seuraavaa:

- Asiakirjan vastaanottaja voi laajentaa jakelua lainsäädännön ja sopimusten sekä suojaustasoon liittyvien rajoitusten puitteissa
- Asiakirjan jakelu määritetään asiakirjan sisältämän tiedon pohjalta niille tahoille, joita asiakirja koskettaa.

Luokiteltu asiakirja voidaan jakaa muille viranomaisille ja sidosryhmille ottamalla huomioon asiakirjan suojaustason, laatijan ja sopimusten asettamat vaatimukset.

8.6 Asiakirjan lähettäminen, siirto ja/tai pääsy tietoon

Kun asiakirja luovutetaan vastaanottajalle, se siirtyy tietosisältöineen vastaanottajan hallintaan kaikkine siihen liittyvine oikeuksineen sekä velvollisuuksineen, jollei erityissäännöksistä muuta johdu.

Suojaustasoa I – III edellyttävä asiakirja osoitetaan henkilölle, määrättyä tehtävää hoitavalle tai organisaatiolle. Lähettäjän on varmistettava, että salassa pidettävä asiakirja luovutetaan vain sellaiselle henkilölle, jolla on tehtäviinsä liittyvä oikeus käsitellä kyseistä asiakirjaa.

Suojaustasoon I tai II luokitellun asiakirjan luovutus on dokumentoitava ja suojaustasoa III edellyttävän asiakirjan luovutus on oltava jäljitettävissä.

Suojaustasoon IV luokiteltuun asiakirjaan sisältyviä tietoja voidaan eräissä tapauksissa käsitellä puhelimessa peitetysti. Luokiteltujen asiakirjojen lähettäminen telefaxilla tulee suorittaa kullekin suojaustasolle asetettujen vaatimusten mukaisesti (liite 4, taulukko5).

Luokitellut asiakirjat toimitetaan vastaanottajalle suojaustason asettamien vaatimusten mukaisesti. Luokiteltu asiakirja tulee jakaa siten, etteivät sivulliset pääse käsiksi suojattavaan tietoon.

Tietojärjestelmissä tietojen jakelu toteutetaan ensisijaisesti tarjoamalla pääsyoikeus tietoon tai sähköpostin välityksellä. Luokiteltuun asiakirjaan sisältyvän tiedon käsittelyn tulee tapahtua käyttöoikeuksien puitteissa ottaen huomioon suojaustasokohtaiset vaatimukset.

Luokiteltuun asiakirjaan sisältyviä tietoja saa käsitellä, siirtää ja taltioida vain sellaisissa tietojärjestelmien ja tietoverkkojen osissa, jotka täyttävät kyseisen suojaustason tietovarantojen käsittelylle asettamat tietoturvavaatimukset.

Viranomaisen tulee ylläpitää menettelyjä, joilla varmistetaan tietojen käsittely koko niiden elinkaaren ajan hyvän tiedonhallintavan toteuttamiseksi.

Asiakirjaan voi sisältyä sekä turvallisuusluokiteltua että muun edun vuoksi salassa pidettävää tietoa. Asiakirjaa tulee tällöin käsitellä asiakirjan sisältämien tietojen edellyttämässä ympäristössä ja asettamin vaatimuksin.

Siirrettäessä kansainvälistä turvallisuusluokiteltua tietoa (esim EU, NATO) sähköisesti tai muilla menetelmillä tulee erikseen varmistua, mitä kahdenkeskisissä turvallisuussopimuksissa (vast.) asiasta on sovittu.

8.7 Vastaanottajan toimenpiteet

Luokitellun asiakirjan vastaanottaja kirjaa vastaanotetun aineiston asiakirjan suojaustasoa vastaavaan diaariin tai rekisteriin. Jos asiakirja tulee suoraan vastaanottajalle, hänen on huolehdittava asiakirjan kirjaamisesta.

Asiakirjan vastaanottaja tarkastaa, että käsittelystä vastaavalla henkilöllä on oikeus käsitellä luokiteltua asiakirjaa.

Asiakirjan vastaanottaja lähettää asiakirjan edelleen asian käsittelijälle käyttäen esim. suljettua kuorta, jos kyseessä on luokiteltu asiakirja, ja muutenkin huomioiden asiakirjojen siirtoon liittyvät menettelytavat.

Salassa pidettävää tietoaineistoa ei saa jättää esille tai valvomatta työtilasta poistuttaessa.

Asiakirjan vastaanottaja vastaa kaikista asiakirjan käsittelyyn liittyvistä velvollisuuksista käsittely- ja käyttöoikeuksineen.

Vastaanotettaessa kansainvälistä turvallisuusluokiteltua tietoa (esim. EU, NATO) sähköisesti tai muilla menetelmillä tulee erikseen varmistua, mitä kahdenkeskisissä turvallisuussopimuksissa (vast.) asiasta on sovittu. Ulkomaiset

asiakirjat merkitään tarvittaessa myös kotimaisilla suojaustaso/turvallisuusluokitusmerkinnöillä

8.8 Asiakirjojen tallettaminen ja säilyttäminen

Julkinen ja luokiteltu asiakirja-aineisto (tieto) tulee pitää erillään.

Luokiteltua tietoa sisältävät asiakirjat tulee säilyttää siten, että vain käyttöoikeuden omaava henkilöstö pääsee käsittelemään kyseistä aineistoa.

Sähköisissä järjestelmissä tulee käyttää suojaustasokohtaiset vaatimukset täyttäviä ratkaisuja.

Luokitellun tiedon säilytyksen valvonta on järjestettävä.

Muisteille talletettavat luokitellut tiedot on suojattava käyttämällä hyväksi suojaustason mukaisia, hyväksyttyjä salausratkaisuja.

Luokitellut (suojaustasot I – III) paperimuotoiset asiakirjat on säilytettävä vähintään Euro II -normin mukaisessa data- tai kassakaapissa sen mukaan, mikä asiakirjan suojaustaso on. Luonnokset eivät tee poikkeusta tästä. Suojaustasoon IV kuuluvat asiakirjat tulee säilyttää lukitussa paikassa.

8.9 Pääsy tietoon

Viranomaisen tulee ylläpitää turvallisia menettelyjä, joiden avulla vain tietoon oikeutetut pääsevät käsittelemään salassa pidettävää tai muun syyn vuoksi suojattavaa tietoa.

Viranomaisen tulee todentaa riittävän vahvalla menettelyllä henkilöt ja/tai palvelua pyytävät tahot tarjotessaan käsittelymahdollisuuden salassa pidettävään tai muun syyn vuoksi suojattavaan tietoon.

8.10 Tietoaineistojen arkistointi

Arkistoinnin tulee pohjautua arkistonmuodostussuunnitelmissa määriteltyihin rakenteisiin ja vaatimuksiin.

Arkistoinnissa on otettava huomioon suojaustason ja sopimusten käsittelylle asettamat ehdot.

Kansainväliseen toimintaan liittyvät asiakirjat tulee arkistoida sopimuksissa määritellyin tavoin.

Pysyvästi arkistoitavien asiakirjojen osalta noudatetaan Arkistolaitoksen määräyksiä.

8.11 Asiakirjojen suojaustason päivittäminen

Viranomaisen tulee arvioida asiakirjojensa suojaustasomääritysten ajantasaisuus antaessaan niistä tietoa niitä pyytäville.

Asiakirjojen uudelleen luokituksesta ja suojaustarpeen lakkaamisesta vastaa asiakirjan laatija ja/tai asiakirjan toimivaltaa käyttävä viranomainen.

8.12 Tietoaineistojen hävittäminen

Tarpeettomat asiakirjakopiot tulee hävittää käyttötarpeen päätyttyä. Hävittämisen suorittaa organisaation siihen valtuuttama henkilö. Asiakirjan valmistelija vastaa valmistelussaan olevien luonnosvaiheen asiakirjojen hävittämisestä.

Aineiston hävittämisessä on varmistauduttava, ettei se joudu oikeudettomien haltuun.

Paperiasiakirjat tuhotaan suojaustasolle asetetut vaatimukset täyttävää menettelyä käyttäen.

Sähköiset tiedostot tuhotaan tietovälineiltä, työasemilta ja palvelimilta sekä muilta laitteilta suojaustason edellyttämällä tavalla. Tietojärjestelmien käytön yhteydessä syntyvät väliaikaistiedostot on poistettava käyttötarpeen päätyttyä tietohallinnon antamien ohjeiden mukaisesti.

Viranomaisen tulee varmistaa, ettei tietojärjestelmä käsittelyn yhteydessä tallenneta luokitusta edellyttävää tietoa työaseman tai palvelinympäristön muistialueeseen, jonne kyseisen tiedon kannalta asiattomilla on pääsymahdollisuus. Tämä vaatimus koskee myös väliaikais- ja muita tallenteita.

Salassa pidettävät paperiasiakirjat on hävitettävä joko polttamalla, silppuamalla tai keräämällä ne lukittuun astiaan, jonka sisältö hävitetään auditoidussa ja valvotussa ympäristössä.

8.13 Asiakirjan antamisesta päättäminen

Tiedon antaminen viranomaisen hallussa olevasta asiakirjasta määräytyy julkisuuslain mukaan. Asiakirjan luokittelumerkintä ei vaikuta viranomaisen velvollisuuteen tapaus- ja asiakirjakohtaisesti arvioida asiakirjan julkisuus silloin, kun joku pyytää asiakirjasta tiedon julkisuuslain nojalla. Kansainvälisistä tietoturvallisuusvelvoitteista tehdyn lain mukaiset merkinnät eivät jätä salassapidolle harkintamahdollisuutta, toisin kuin julkisuuslain mukaiset merkinnät.

Asiakirjan antamisesta päättää yleisen säännön mukaan se viranomainen, jonka hallussa asiakirja on. Viranomainen voi kuitenkin siirtää tiedonsaantipyynnön sille viranomaiselle, joka on laatinut asiakirjan tai jonka käsiteltävään

asiaan se kuuluu. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan turvallisuusluokitellun asiakirjan saantia koskeva pyyntö on aina siirrettävä sille viranomaiselle, jolle sopimuspuoli on asiakirjan toimittanut. Siirto on pakollinen myös silloin, kun pyyntö koskee asiakirjoja joihin on valtioneuvoston erikseen antamien säännösten mukaan pakko tehdä turvallisuusluokitusta koskeva merkintä. Tällaisia säännöksiä ei ole toistaiseksi annettu.

Julkisuuslain salassapitosäännökset estävät tiedon antamisen sivulliselle. Laissa tarkoitettuna sivullisena ei pidetä sitä, jonka tehtäviin asian käsittely viranomaisessa kuuluu. Julkisuuslain 26 §:n 3 momentin mukaan tietoja voidaan lainkohdassa säädetyin edellytyksin antaa myös sille, joka toimii viranomaisen toimeksiannosta. On syytä huomata, että viranomaisten toimeksiannosta toimivat ovat suoraan julkisuuslain 23 §:n 2 momentin mukaan vaitiolovelvollisia, joten salassapitovelvollisuus on olemassa ilman erillistä vaitiolositoumustakin. Salassapitovelvollisuudesta on kuitenkin aina informoitava toimeksiantotehtävän saanutta ja tämän palveluksessa olevia.

Jos on välttämätöntä antaa luokiteltuja tietoaineistoja toimeksiantotehtävää suorittavalle, on varmistauduttava etukäteen siitä, että toimeksiantotehtävää suorittavalla on käytössään tarvittavat käsittelyn edellyttämät tilat sekä asianmukaiset menettelyt ja tieto viranomaisen käsittelyvaatimuksista. Sopimukseen on syytä sisällyttää nimenomaiset määräykset tiedonkäsittelyn asianmukaisuuden varmistamiseksi.

Henkilötietojen käsittelytehtäviä voidaan antaa ulkomailla suoritettaviksi vain henkilötietolaissa säädetyin edellytyksin. Valmisteilla on säännökset yritysturvallisuus-selvityksistä, joiden käyttämistä on syytä harkita aina, jos laajoja ja yhteiskunnan toimintojen kannalta keskeisten tietoaineistojen käsittelytehtäviä annetaan julkishallinnon ulkopuolelle.

Asiakirjan salassapitovelvollisuus on riippuvainen ajankohdasta, josta käsin asiaa tarkastellaan. Turvallisuus- tai suojaustasoa ilmoittava salassapitomerkintä osoittaa tilanteen silloin, kun tietoaineisto laaditaan. Salassapitovelvollisuus ja tietoturvallisuutta koskevat vaatimukset voivat muuttua ajan kuluessa. Tämän vuoksi tiedonsaantipyyntöä ratkaistaessa on selvitettävä, onko perusteita suojaustasoluokitukselle ja salassapidolle edelleen olemassa. Jos kysymys on kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvista asiakirjoista, on tarpeen ottaa yhteyttä asiakirjan laatineeseen sopimusosapuoleen tai järjestöön.

8.14 Salauksen vaikutus tietoaineistojen käsittelyyn

Salausmenetelmien avulla tiedon esitystapa muutetaan ei-ymmärrettävään muotoon. Tieto saadaan takaisin selväkieliseen muotoon oikean lisätiedon (salausavaimen) avulla. Salausmenetelmiä voidaan käyttää myös tiedon eheyden varmistamiseen.

Tyypillisiä käyttökohteita ovat tiedon tallennukseen käytettävät ulkoiset muistit, kannettavien työasemien kiintolevyt, verkkopalvelut ja sähköposti. Suojaamalla näiden laitteiden muistien sisältämät tiedot ja tietoliikenne salaustekniikan avulla varmistutaan, ettei niiden sisältämä tieto paljastu ulkopuolisille edes laitteiden anastamis- ja katoamistilanteissa.

Suojaustasoon I kuuluva tieto tulee aina olla vahvasti salattu tai muutoin vahvasti suojattu, kun sitä taltioidaan tai käsitellään ainoastaan valvotuissa erillisverkoissa. Suojaustasoon II kuuluva tieto tulee olla vahvasti salattu kun sitä siirretään tai käsitellään perus- tai korotetun tason tietojenkäsittely-ympäristössä. Suojaustasoon III kuuluva tieto voidaan tallettaa selväkielisessä muodossa valvotuissa korotetun tai korkean tietoturvallisuustason verkon palvelimilla. Muissa verkkoympäristöissä suojaustason III tietoa saadaan siirtää ja tallettaa vain asianmukaisesti salattuna. Myös suojaustasoon IV kuuluva tieto tulee salata, kun sitä siirretään ja taltioidaan yleisessä verkossa ja sen palvelimilla, ellei lähettäjän ja vastaanottajan kesken ole sovittu muusta turvallisesta järjestelystä.

Tiedon salaaminen voi olla vahvaa tai heikkoa. Erilaisilla salausmenetelmillä saadaan eritasoisia salaustuloksia. Käytettäessä vahvaa salausmenetelmää voidaan tietoaineiston tulkinnan arvioida kestävän riittävän pitkään.

Salassa pidettävää tietoa saa siirtää ja taltioida vain viranomaisen hyväksymillä salausmenetelmillä (vast.) suojattuna. Erityistä huolta tulee pitää salauksessa käytettävien salasanojen ja työvälineiden turvallisuudesta.

Riittävän vahvasti salattua asiakirjaa voidaan käsitellä kuten julkista asiakirjaa.

LIITTEET

Liite 1. Lainsäädännön asettamat velvoitteet

Lainsäädäntökatsaus tietoturvallisuuden osalta löytyy Yleisohje tietoturvallisuuden johtamiseen ja hallintaan -ohjeesta (VAHTI 3/2007).

Tämän ohjeen kannalta keskeiset normiohjaukseen liittyvät kohdat:

Suomen lainsäädännöstä

- Julkisuuslaki (625/1999):
  Hyvä tiedonhallintatapa, tietoturvatyön perusteet, salassapito- ja vaitiolovelvollisuus, salassapitomerkinnät, luokituksen perusteet
- Julkisuusasetus (1030/1999):
  Selvitykset ja arvioinnit hyvän tiedonhallintatavan toteuttamiseksi
  Diaarit ja muut asiakirjarekisterit
- Tietoturvallisuusasetus (681/2010)
  Tietoturvallisuuden yleiset lähtökohdat, asiakirjojen luokittelu ja käsittelyvaatimukset
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
  Kansainvälisen aineisto käsittely
- Henkilötietolaki (523/1999)
  Hyvä tietojenkäsittelytapa, käyttötarkoitussidonnaisuus, suojausvelvoite
- Henkilötietojen käsittelyä koskevat erityislait
- Arkistolaki
  Asiakirjahallinto ja arkistotoimi
- Erityislainsäädäntö

Lisää normiohjauksesta FINLEX :sta (www.finlex.fi).

Suomea sitovista kansainvälisistä tietoturvallisuusvelvoitteista

- Suomen ja NATO:n välinen PFP asiakirjaturvallisuussopimus 22.9.1994
- Suomen ja WEU:n välinen turvallisuussopimus 22.4.1997 (SopS 42/1998)
- EU neuvoston päätös neuvoston turvallisuussääntöjen vahvistamisesta (2001/264/EY)
- Euroopan avaruusjärjestön (ESA) yleissopimus turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta (SosO 95/2004)
- Suomea sitovat kahdenväliset tietoturvallisuussopimukset: esim. Saksan, Ranskan, Slovakian, Viron, Italian ja Puolan kanssa

Lisätietoja kansainvälisistä sopimuksista on osoitteessa:www.formin.fi

Liite 2. Salassa pidettävien asiakirjojen ja tietojen leimat

Salassapitoleima ja suojaustasomerkintä

SALASSA PIDETTÄVÄ
Suojaustaso __
JulkL (621/1999) 24.1 §:n _____k
Lain (___/_____) ___ §:n _____k

SALASSA PIDETTÄVÄ -leimalla voidaan tarvittaessa ilmoittaa suojaustaso. Leimaan kirjoitetaan käsin / 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, jotka sisältävät viranomaisharkintaan tai käyttötarkoitussidonnan alaista luokiteltavaa tietoa.

Turvallisuusluokitusmerkintöjen leimat

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24.1 §:n _____k
L (____/_____) ____ §:n ____k

LUOTTAMUKSELLINEN
Suojaustaso III
JulkL (621/1999) 24.1 §:n _____k
L (____/_____) ____ §:n ____k

ERITTÄIN SALAINEN
Suojaustaso I
JulkL (621/1999) 24.1 §:n _____k
L (____/_____) ____ §:n ____k

SALAINEN
Suojaustaso II
JulkL (621/1999) 24.1 §:n _____k
L (____/_____) ____ §:n ____k

Salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä. Turvallisuusluokitusmerkintää saadaan käyttää vain niiden salassa pidettävien asiakirjojen kohdalla, jotka ovat salassa pidettäviä julkisuuslain 24.1 §:n kohtien 2 ja 7-10 tai kansainvälisistä tietoturvallisuusvelvoitteista annetun lain perusteella. Kansainvälisiin turvallisuusluokiteltuihin aineistoihin on tehtävä aina turvallisuusluokkaa osoittava merkintä (588/2004, 8 §).

Liite 3. Yksityiskohtaiset ohjeet viranomaiselle asiakirjojen turvallisen käsittelyn mahdollistamiseksi

Tässä asiakirjaliitteessä esitetään yksityiskohtaisia ohjeita viranomaiselle tarvittavista toimenpiteistä, joilla luodaan turvallinen toimintaympäristö kaiken salassa pidettävän tiedon, niin kotimaisen kuin ulkomaisen käsittelyn mahdollistamiseksi. Vaatimukset on esitetty pääasiakirjan (luku 4) esittämässä järjestyksessä.

1 Yleiset vaatimukset kaikilla suojaustasoilla

(1) Viranomaisen tulee ylläpitää menettelyjä, joilla varmistetaan asiakirjojen ja tietojen hallittu käsittely koko asiakirjan elinkaaren ajan. Tämän menettelyn tulee tapahtua hyvän tiedonhallintatavan mukaisin toimenpitein.

(2) Menettelyn tulee pohjautua viranomaisen ylläpitämään prosessipohjaiseen arkistonmuodostussuunnitelmaan.

(3) Käsittelysäännöillä pyritään varmistamaan, että salassa pidettävät tiedot pysyvät vain niiden käytössä, joilla on oikeus käsitellä tietoja (luottamuksellisuus). Samalla varmistetaan, että tiedot ovat käytettävissä (käytettävyys) ja oikeita (eheys).

(4) Asiakirjoja on suojattava niin kauan, kuin ne lain ja Suomea sitovien sopimusten ja säädösten sekä aineiston laatineen ilmoituksen mukaan ovat tarkoitetut turvallisuustoimenpiteiden kohteeksi.

(5) Viranomaisen tulee huolehtia siitä, että viranomaisen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta, tietojen antamisessa ja käsittelyssä noudatettavasta menettelystä sekä asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, turvallisuusjärjestelyistä ja tehtävänjaosta.

(6) Viranomaisen tulee antaa tarvittava lisäohjeistus ja koulutus. Osaamista on seurattava.

(7) Viranomaisen tulee valvoa säännönmukaisesti arkaluonteisten tietoaineistojen tietoturvatoimenpiteiden toteuttamista sekä seurattava annettujen ohjeiden ja teknisten tietoturvatoimenpiteiden toimivuutta.

2 Henkilöstöä koskevat vaatimukset

(1) Henkilön tulee tuntea ja hallita käyttämiensä työvälineiden käyttötavat ja ohjeisto.

(2) Henkilön tulee hallita salassa pidettävien asiakirjojen käsittelysäännöt.

(3) Käsittelyoikeudet tulee sitoa työtehtävään. Oikeuksien tulee perustua esimiehen päätökseen.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(4)	Kun henkilön oikeus aineiston hallussa pitämiseen muuttuu, tulee kyseinen aineisto tuhota tai luovuttaa pois organisaation johdon määrittelemällä tavalla.	kyllä	kyllä	kyllä	kyllä
(5)	Käsittelyoikeuden myöntäminen edellyttää perusmuotoisen turvallisuusselvityksen suorittamista.	ei	kyllä *	kyllä	kyllä
(6)	Viranomaisen tulee ylläpitää luetteloa luokitellun tiedon käsittelyoikeuksista:				
	kotimainen tietoaineisto	ei	ei	kyllä	kyllä
	kansainvälinen tietoaineisto		sopimuksen mukaan	kyllä	kyllä
(7)	Käsittelyoikeus edellyttää tietoturvallisuuden osaamistestin läpäisyä	suositellaan	kyllä, käsiteltäessä tietoa verkkoympäristössä	kyllä	kyllä

* Organisaatio päättää erikseen henkilöryhmät, joista tehdään perusmuotoinen turvallisuusselvitys. Kansainväliset sopimukset asettavat myös velvotteita luokiteltua tietoa käsittelevien henkilöiden turvallisuusselvitysten suhteen.

3 Tietoturvakulttuuria koskevat vaatimukset

(1) Viranomaisen tulee ylläpitää koko henkilökunnalle tarkoitettua tietoturvakoulutusta ja varmistua henkilöstön riittävästä osaamisesta ja tietoturvallisuuteen liittyvien riskien ymmärtämisestä.

(2) Katso tarkentavat tiedot ohjeen luvun 4.3 kohdalta.

4 Tilaturvallisuutta koskevat vaatimukset

(1) Tilaturvallisuuden tarkoituksena on osana fyysistä turvallisuutta suojata henkilöstöä, tietoja ja materiaalia.

(2) Viranomaisen on määriteltävä toimi- ja laitetilojensa turvallisuusratkaisut. Ohjeistuksessa on määriteltävä vaadittavat rakenteelliset ratkaisut, tarvittavat valvontajärjestelmät ja mahdollisesti tilan käyttöoikeuksiin liittyvät asiat.

(3) Viranomainen vastaa tietotyössä käytettävien tilojen turvallisuudesta.

Katso tilaturvallisuuteen liittyvä kuvaus pääasiakirjan luvusta 4.4.

5 Tietotekniselle ympäristölle ja tietopalveluille asetettavia vaatimuksia

5.1 Tietoteknisen ympäristön toteuttaminen ja ylläpito

(1) Viranomaisen on suunniteltava ja ylläpidettävä tietojärjestelmänsä ja tietopalvelut siten, että viranomaisen toimintaprosessien edellyttämä tietojenkäsittely on mahdollista suorittaa hyvän tiedonhallintatavan mukaisesti kaikissa toimintatiloissa. Tietojenkäsittely-ympäristöt luokitellaan kuuluvaksi perus-, korotetun ja korkean tietoturvallisuustason ympäristöiksi sen mukaan, miten ne täyttävät eri turvallisuustasoille asetetut teknilliset ja hallinnolliset vaatimukset (katso liite 5).

(2) Tilat luokitellaan 4 eri tilaluokkaan (turvallisuusvyöhykkeeseen). Suojaustasoihin I - III kuuluvaa tietoa sisältävissä tiloissa tulee olla mm. jatkuva kulunvalvonta, rikosilmoitinjärjestelmä sekä dokumentoitu lukitusjärjestely. Edellä mainituissa tietoteknisissä ympäristöissä on huomioitava sähkömagneettisen hajasäteilyn uhkatekijät.

Katso tietoteknistä ympäristöä koskeva kuvaus pääasiakirjan luvusta 5.

5.2 Tietopalvelujen toteuttaminen

Viranomaisen on suunniteltava ja ylläpidettävä asiakirjojen rekisteröinnin mahdollistavia rakenteita, joiden avulla mahdollistetaan tietojen suojaaminen sekä niiden käytettävyyden, eheyden ja luotettavuuden varmistaminen. Vaikka näiden edellä mainittujen tavoitteiden toteuttaminen tapahtuu sähköisessä toimintaympäristössä osin tietoturvallisuutta ja tietoteknisiä ratkaisuja kehittämällä, kyse on viime kädessä hyvästä suunnittelusta sekä näitä tukevien organisaation toimintatapojen kehittämisestä.

Oheiseen taulukkoon on kirjattu eräitä olennaisia vaatimuksia tietopalvelujen toteuttamiseksi suojaustasoittain. Tarkempi luettelo vaatimuksista on esitetty liitteessä 4.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Salassa pidettävä tietoaineisto tulee säilyttää koko salassapitoajan vain tietoon oikeutettujen saatavilla. Tilojen käyttöä on valvottava kulunvalvonnalla ja muilla toimenpiteillä.	kyllä	kyllä	kyllä *	kyllä *
(2)	Tietojärjestelmien tietovarannoista otettuja varmuustallenteita tulee käsitellä kuten alkuperäisiä asiakirjoja. Varmuustallenteiden suojaustaso määräytyy tallenteen sisältämän tiedon korkeimman suojaustasoluokan mukaisesti.	kyllä	kyllä	kyllä	kyllä
(3)	Työtila, jossa on salassa pidettävää tietoa, tulee lukita tilasta poistuttaessa ja/tai estää muutoin sivullisten mahdollisuus käsitellä kyseistä tietoa.	kyllä	kyllä, lisäksi suositellaan asiakirjojen siirtämistä kassakaappiin Kansainväliset asiakirjat tulee säilyttää kassakaapissa	kyllä, lisäksi asiakirjat on siirrettävä kassakaappiin	kyllä, lisäksi asiakirjat on siirrettävä kassakaappiin (tietokone tai tietoväline)
(4)	Salassa pidettävän sähköisen tietoaineiston käsittelyn tulee kirjautua sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai itse asiakirjaan.	suositellaan, kyllä henkilötietojen osalta (HetiL 11§)	suositellaan, kyllä arkaluonteisten henkilötietojen osalta	kyllä	kyllä
(5)	Salassa pidettävän tietoaineiston käsittely avoimissa tietoverkossa.	salattuna tai suojattuna avoimissa tietoverkoissa	salattuna tai suojattuna avoimissa tietoverkoissa	vahvasti salattuna tai vahvasti suojattuna avoimissa tietoverkoissa	käsittely ei sallittu avoimissa tietoverkoissa.
(6)	Salassa pidettävän tietoaineiston käsittely viranomaisen tietoverkossa.	selväkielisenä käyttövaltuuden tarkistavassa, perustietoturvallisuustason tietoverkossa	selväkielisenä korotetun tai korkean tietoturvallisuustason tietoverkoissa	selväkielisenä valvotuissa korkean tietoturvallisuustason vaatimukset täyttävissä tietoverkoissa	sallittu vahvasti suojattuna erillisverkossa, joka täyttää korkean tietoturvallisuustason vaatimukset ja johon ei ole yhteyttä muista tietoverkoista
(7)	Salassa pidettävän tietoaineiston tallentaminen viranomaisen tietoverkoissa	perustietoturvallisuustason palvelemilla voidaan tallentaa selväkielisenä suojattuna käyttäjätunnuksilla, suositellaan salausta,	perustietoturvallisuustason palvelimilla salattuna tai suojattuna; korotetun ja korkean tietoturvallisuustason palvelimilla sallitaan selväkielisenä	vahvasti salattuna tai vahvasti suojattuna, jos järjestelmä täyttää korkean tietoturvallisuuden tason vaatimukset.	sallittu vahvasti suojattuna valvotussa erillisverkossa joka täyttää korkean tietoturvallisuustason vaatimukset.
(8)	Salassa pidettävän tietoaineiston käsittely sähköisessä muodossa työpaikan ulkopuolella Käsittely edellyttää kaikissa luokissa viranomaisen päätöstä (vrt TTA 16 §)	sallittu, tieto tulee suojata, esimerkiksi salausta käyttäen	sallittu, tieto tulee tallentaa salattuna	erillishyväksyntä, tieto tulee tallentaa vahvaa salausta käyttäen	ei sallittu ilman tapauskohtaista viranomaispäätöstä

* Tietoa saa säilyttää vain sellaisissa tiloissa, jotka ovat valvotun ja dokumentoidun kulunvalvonta- ja lukitusjärjestelyn piirissä ja jotka kuuluvat luokiteltuihin turva-alueisiin.

5.3 Asiakirjan antamisesta päättäminen

(1) Tiedon antaminen viranomaisen hallussa olevasta asiakirjasta määräytyy julkisuuslain mukaisesti.

(2) Viranomaisen on määriteltävä, kenen asiana on ratkaista julkisuuslain nojalla tehdyt pyynnöt saada tieto luokitellusta asiakirjasta. Asianmukaisinta on osoittaa tämä tehtävä esimiesasemassa olevalle virkamiehelle, jollei erityisistä syistä muuta johdu.

(3) Luokiteltuihin tietoaineistoihin sisältyvien tietojen luovuttamista toimeksiantotehtävää varten edellytyksenä on, että tiedonsaaja tuntee luokiteltujen tietoaineistojen käsittelysäännöt ja lain sekä sopimusten asettamat vaatimukset.

Kun viranomaisella on toimeksiantoihin liittyen tarve luovuttaa luokiteltua tietoa, tulee etukäteen varmistua, että

(a) viranomaisella on tiedonsaajan voimassa oleva, asiakirjojen luokkaa vastaavat turvallisuusjärjestelyt kattava turvallisuussopimus
(b) tiedonsaaja ja sen palveluksessa olevat ovat antaneet vaitiolovakuutuksen, milloin kansainvälinen sopimus tai säädös sitä edellyttää
(c) tietoja saavat ja niitä käsittelevät tuntevat näiltä osin viranomaisen käsittelysäännöt.

(4) Asianmukaista on, että luokiteltuun tietoaineistoon sisältyvän asiakirjan tiedonsaantipyyntöä koskeva tiedonsaantipyyntö siirretään sille viranomaiselle, jonka käsiteltäväksi asia kokonaisuudessaan kuuluu (julkisuuslaki 15 §).

(5) Luokiteltuun tietoaineistoon kuuluvia tietoja sisältävien asiakirjapyyntöjen käsittelyssä on varmistettava, onko perusteita edelleen pitää voimassa tietoaineistojen luokitus ja salassapito.

Liite 4. Salassa pidettävien asiakirjojen ja tietojen käsittelyvaatimukset

Tässä liitteessä esitetään yksityis-kohtaiset käsittelyohjeet salassa pidettävää tietoa sisältävien asiakirjojen osalta. Käsittelyvaatimukset on esitetty taulukkomuodossa suojaustasoittain.

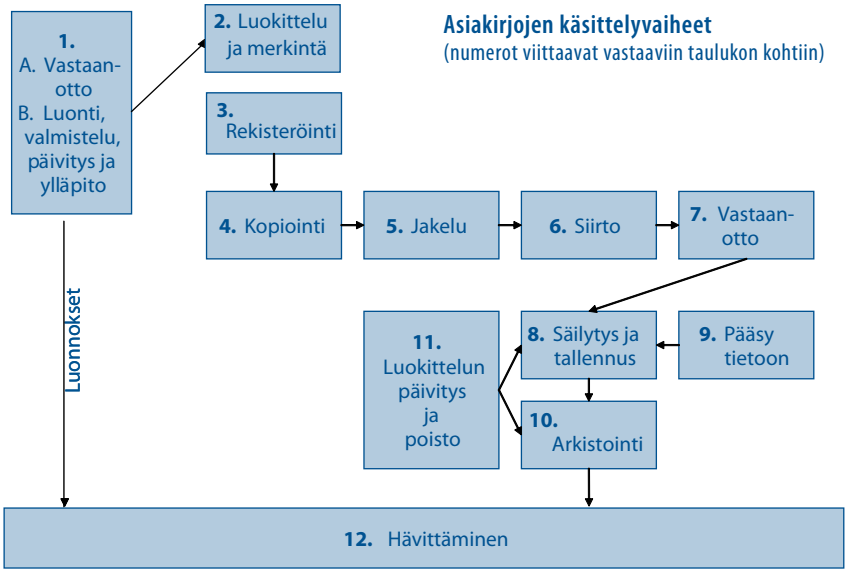
Vaatimukset on ryhmitelty elinkaaren eri vaiheisiin.

Oheisessa kuvassa on esitetty tyypillinen asiakirjan käsittelyprosessi ja sen vaiheet. Tiedon käyttäjän osuus liittyy erityisesti kohtaan 'Pääsy tietoon'.

Kuviossa ei ole esitetty kaikkia erilaisia tilanteita, joita tiedon käyttäjän eteen tulee erilaisissa työtehtävissä.

Luokituksen päivittäminen ja poisto tehdään tekemällä tähän liittyvä esitys sen uudelleen arviointia varten.

Arkistoissa olevien asiakirjojen julkisuutta ohjaa salassa pitoa koskeva lainsäädäntö.



Koko elinkaarta koskevat vaatimukset

Tässä esitetään yleiset käsittelyohjeet asiakirjoille, jotka edellyttävät suojaustason mukaista käsittelyä. Nämä ohjeet koskevat tiedon koko elinkaarta. Seuraavissa luvuissa vaatimukset ovat yksityiskohtaisempia ja koskevat kyseisiä käsittelyvaiheita.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Asiakirjojen suojaustaso-kohtaiset vaatimukset tulee ottaa huomioon koko elinkaaren ajan.	kyllä	kyllä	kyllä	kyllä
(2)	Viranomaisen asiakirjasta tulee käydä ilmi riittävät asiakirjan yksilöimiseen liittyvät tunnisteet.	kyllä	kyllä	kyllä	kyllä
(3)	Asiakirjoja tulee käsitellä huolella siten, että vain ne, joilla on siihen oikeus, pääsevät käsiksi salassa pidettävään tietoon. Asiakirjojen suojaaminen tulee varmistaa erityisesti tilanteissa, joissa samassa tilassa on henkilöitä, joilla ei ole käsittelyoikeutta kyseessä olevaan tietoon.	kyllä	kyllä	kyllä	kyllä
(4)	Kansainvälisten asiakirjojen osalta noudatetaan kansainvälistä sopimusta, jos sellainen on saatettu lailla voimaan. Muissa tilanteissa noudatetaan Suomen lakia.	kyllä	kyllä	kyllä	kyllä
(5)	Asiakirjojen käsittelyvaatimukset ovat riippumattomia siitä, missä muodossa tieto on tallennettu tai esitetty.	kyllä	kyllä	kyllä	kyllä
(6)	Asiakirjoja on käsiteltävä arkistonmuodostussuunnitelman mukaisesti.	kyllä	kyllä	kyllä	kyllä
(7)	Asiakirjoja ei saa jättää esille tai ilman valvontaa työtilasta poistuttaessa. Suojaustason IV asiakirjoja voi jättää tilapäisesti esille ottaen huomioon tilajärjestelyt ja käytössä olevat lukitukset.	kyllä	kyllä	kyllä	kyllä
(8)	Asiakirjojen käsittelyssä on otettava huomioon käsittely-ympäristölle asetetut luokkakohtaiset vaatimukset.	kyllä	kyllä	kyllä	kyllä
(9)	Asiakirjojen käsittelyssä on otettava huomioon henkilöstöturvallisuudelle asetetut vaatimukset (käsittelyoikeuden edellytykset ja käsittelysääntöjen osaaminen).	kyllä	kyllä	kyllä	kyllä

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(10)	Asiakirjojen käsittelyä työpaikan ulkopuolella tulee välttää. Mikäli työtehtävät sitä kuitenkin edellyttävät, tulee asiakirjoja käsitellä tässä ohjeessa annettujen periaatteiden ja vaatimusten mukaisesti.	kyllä	kyllä	kyllä	kyllä
(11)	Asiakirjojen käsittelystä tulee jäädä merkintä, mikä mahdollistaa asiakirjan ja siitä otettujen kopioiden seurannan suojaustarvetta edellyttävältä ajalta.	Ei edellytetä paitsi henkilötietojen osalta	Suositellaan, pakollinen arkaluonteisten henkilötietojen osalta	Lokitieto tai kuittauslista käsittelystä	Täydellinen, kopiokohtainen jälki asiakirjaan tutustuneista

1 Asiakirjojen luonti ja vastaanotto

Tietojen vastaanotolla (1a) tarkoitetaan tässä niitä tilanteita, joissa organisaatio vastaanottaa muualla tuotettuja asiakirjoja.

Asiakirjojen luontivaiheella (1b) tarkoitetaan niitä käsittelyvaiheen jaksoja, jolloin tietoaineistoon tuodaan uutta tietoa tai tehdään päivityksiä. Usein tiedon tuottajana on henkilö, mutta myös erilaiset tietojärjestelmien käsittelyprosessit voivat tuottaa automaattisesti tietoa erilaisiin tietovarantoihin.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Kerättäessä ja luovutettaessa tietoaineistoa sekä valmisteltaessa ja luotaessa asiakirjaa on otettava huomioon asiakirjan julkisuudesta ja salassa pidosta annettu lainsäädäntö, arkistonmuodostussuunnitelman vaatimukset sekä viranomaisten antamat ohjeet.	kyllä	kyllä	kyllä	kyllä
(2)	Valmistelutyössä tulee ottaa kaiken aikaa huomioon, että aineisto koko käsittelyprosessin ajan käsitellään ympäristössä, jossa vain ne, joilla on aineiston käyttöoikeus, pääsevät siihen.	kyllä	kyllä	kyllä	kyllä
(3)	Valmisteltaessa tietoaineistoa tulee eri turvaluokkiin kuuluvat tiedot esittää mahdollisuuksien mukaan eri asiakirjoissa.	kyllä	kyllä	kyllä	kyllä
(4)	Viranomaisen asiakirja on rekisteröitävä tai muulla tavoin hallittava	kyllä	kyllä	kyllä	kyllä

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(5)	Kansainväliset turvallisuusluokitellut asiakirjat leimataan vastaavilla kotimaisilla turvallisuusluokkaa osoittavilla leimoilla, jos niin on Suomea sitovassa sopimuksessa määrätty tai jos Suomen laki sitä muutoin edellyttää. Kansainvälisiin turvallisuusluokiteltuihin aineistoihin on tehtävä aina turvallisuusluokkaa osoittava merkintä (588/2004, 8 §).	kyllä	kyllä	kyllä	kyllä
(6)	Tietojärjestelmissä, jotka tuottavat automaattisesti tietoa, kuten valvontatietoa tai lokitietoa tai muuta salassa pidettävää tietoa, tulee käsittelijän varmistua myös omasta oikeudestaan tietoon.	kyllä	kyllä	kyllä	kyllä

2 Asiakirjojen luokittelu ja merkintä

Asiakirjojen luokittelulla tarkoitetaan niitä toimenpiteitä, jotka tarvitaan määriteltäessä asiakirjalle tai tiedolle oikea suojaustaso. Merkinnällä tarkoitetaan asiakirjaan tehtävän suojaustason tai turvallisuusluokkaa osoittavan leiman (liite 2) tuottamista.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Salassa pidettävät asiakirjat tulee luokitella lakien ja asetuksen mukaisesti.	kyllä	kyllä	kyllä	kyllä
(2)	Tiedon luokittelee se henkilö, joka antaa asiaan liittyvän toimeksiannon tai ensimmäisen kerran luo tiedot tai henkilö, joka päättää asiakirjan luokittelusta. Huomaa laki kansainvälisistä tietoturvallisuusvelvoitteista.	kyllä	kyllä	kyllä	kyllä
(3)	Merkinnän käsittelyluokasta tekee asiakirjan laatija tai ensimmäinen vastaanottaja tai se, jolla on oikeus päättää kyseisen tiedon käsittelystä ja käytöstä.	kyllä	kyllä	kyllä	kyllä
(4)	Luokittelun vahvistaa asiakirjan allekirjoittaja manuaalisella tai sähköisellä allekirjoituksellaan. Kaikella tiedolla ei ole välttämättä allekirjoittajaa.	kyllä	kyllä	kyllä	kyllä

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(5)	Asiakirjat merkitään asiakirjan osien ylintä suojaustasoa vastaavalla leimalla. Asiakirjat suositellaan laadittaviksi siten, että eri suojaustasoihin kuuluvat tiedot esitetään omissa asiakirjoissa.	kyllä	kyllä	kyllä	kyllä
(6)	Salassa pidettävät asiakirjat tulee varustaa asianomaisin leimoin tai vastaavin merkinnöin, kun organisaatio on päättänyt niiden käytöstä.	kyllä	kyllä	kyllä	kyllä
(7)	Leima sijoitetaan ensimmäisen sivun oikeaan yläkulmaan.	kyllä	kyllä	kyllä	kyllä
(8)	Leima sijoitetaan myös asiakirjan muille sivuille.	ei edellytetä	ei edellytetä	kyllä	kyllä
(9)	Leiman väri on punainen	ei edellytetä	ei edellytetä	kyllä	kyllä
(10)	Käytetään punaisella poikkiviivalla merkittyä paperia tai vastaavan merkinnän toteuttavaa tulostustapaa.	ei	ei	kyllä	kyllä
(11)	Asiakirjan sivut numeroidaan ja sivujen lukumäärä merkitään.	ei edellytä	kyllä	kyllä	kyllä
(12)	Metatietorakenteen sisältävissä asiakirjoissa turvallisuusluokka ilmaistaan vastaavalla lyhenteellä.	ei edellytetä RAJ (R)	kyllä LUOT (L)	kyllä SAL (S)	kyllä ERSAL(E)
(13)	Tietoja sähköisesti käsiteltäessä tulee näytöissä näkyä kulloinkin käsiteltävän tiedon luokitus liitteen 2 merkinnöin.	suositellaan *	suositellaan *	kyllä	kyllä
(14)	Kotimaisen leiman asiakirjaan lisää se organisaatio, joka saa asiakirjan ulkomaiselta taholta.	ei edellytetä	suositellaan	kyllä	kyllä

* Ei edellytetä sellaisissa tietojärjestelmissä, joissa käyttöoikeudet on rajattu vain kyseistä tietoa käsitteleville, ei myöskään sellaisissa valvonta- ja turvallisuusalan ja vastaavissa tietojärjestelmissä, joissa käsitellään pääsääntöisesti salassa pidettävää tietoa ja joissa käyttöoikeudet on rajattu vain kyseiseen tietoon oikeutetuille.

3 Rekisteröinti

Asiakirjan rekisteröinnillä tarkoitetaan tässä yhteydessä niitä toimenpiteitä, joilla asiakirja merkitään diaariin tai vastaavaan rekisteriin, jonka avulla voidaan seurata viranomaisen tietovarantoa.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Asiakirjat kirjataan suojaustason mukaisesti sitä varten määriteltyyn diaariin tai rekisteriin.*	suositellaan	suositellaan	kyllä	kyllä **
(2)	Diaarissa ja rekisterissä suositellaan käytettäväksi suojaustason lyhennettä.	ST IV	ST III	ST II	ST I
(3)	Diaarissa ja rekisterissä suositellaan käytettäväksi turvallisuusluokituksen lyhennettä.	RAJ (R)	LUOT (L)	SAL (S)	ERSAL (E)

* Asianhallintajärjestelmissä diaaritieto (rekisteritieto) sisältää tiedon asiakirjan suojaustasosta. Tällaisen diaarin avulla voidaan tarvittaessa eri näkymillä tarjota eri suojaustasoihin kuuluvat asiakirjaluettelot. Diaarin julkiseen osaan talletettavan tiedon tulee olla julkista. Salassa pidettävät diaarit tulee toteuttaa siten, että vain käyttöoikeuden omaavat pääsevät käsittelemään niitä.
** Suojaustasoon I kuuluvia asiakirjoja varten tulee ylläpitää erillistä diaaria tai rekisteriä.

4 Kopiointi

Tietoaineistojen kopioinnilla tarkoitetaan niitä toimenpiteitä, joilla alkuperäisestä asiakirjasta otetaan jäljennöksiä. Näitä ovat esimerkiksi valokopiointi ja tiedostojen kopiointi eri muistivälineille sekä asiakirjoista tai tietoaineistoista otetut otteet.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Kopioita käsitellään kuten alkuperäistä asiakirjaa.	kyllä	kyllä	kyllä	kyllä
(2)	Sähköisten asiakirjakopioiden osalta tulee varmistua asiakirjan identtisyydestä (eheyden varmistaminen).	kyllä	kyllä	kyllä	kyllä
(3)	Alkuperäisestä asiakirjasta voidaan ottaa sekä sähköisiä että paperimuotoisia kopioita.	kyllä	kyllä	kyllä; jäljitettävyys tulee varmistaa	ei ilman laatijan lupaa, jäljitettävyys tulee varmistaa
(4)	Kopiot on leimattava alkuperäistä asiakirjaa vastaavalla leimalla (kopioituva leima riittää, myös mustavalkoinen leima).	alkuperäinen riittää	alkuperäinen riittää	leimattava punaisella leimalla	leimattava punaisella leimalla

5 Jakelu

Asiakirjojen jakelulla tarkoitetaan niitä toimenpiteitä, joilla päätetään asiakirjan vastaanottajat, varmistetaan vastaanottajien tiedontarve, oikeus ja kyky käsitellä jaettavaa asiakirjaa (salassa pidettävää tietoaineistoa).

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Asiakirjan allekirjoittaja määrää jakelun ja käsittelyprosessin.	kyllä	kyllä	kyllä	kyllä
(2)	Asiakirjasta tulee käydä ilmi, kenelle asiakirja tai sen osat jaetaan. Esim. meta- ja tietokantatietojen osalta tulee käydä ilmi asiakirjan sisältämän tiedon suojaustaso ja jakelu.	kyllä	kyllä	kyllä	kyllä
(3)	Asiakirjan jakelu määritetään asiakirjan sisältämän tiedon pohjalta niille tahoille, joita asiakirja koskettaa.	kyllä	kyllä	kyllä	kyllä
(4)	Jakelu tulee osoittaa organisaatiolle, jolloin varmistutaan asiakirjan rekisteröinnistä. Jakelutiedoissa voidaan käyttää myös henkilönimeä tai tehtävää.	kyllä	kyllä	kyllä	kyllä
(5)	Salassa pidettävän asiakirjan luovutus on dokumentoitava.	ei edellytetä	kyllä	kyllä	kyllä
(6)	Asiakirjan luovuttamisen edellytyksenä on, että laissa on säädetty oikeus tiedon luovuttamiseen ja vastaanottajalla on tarvittavat oikeudet aineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti. *	kyllä	kyllä	kyllä	kyllä
(7)	Kansainvälisten asiakirjojen jakelu toteutetaan kansainvälisten sopimusten ja/tai asiakirjan asettamien vaatimusten mukaisesti.	kyllä	kyllä	kyllä	kyllä

* Asiakirjat luovutetaan yleensä organisaatiolle. Viranomaisten kesken toimittaessa on syytä varmistua vastaanottajan tarpeesta tietoon sekä vastaanottavan tahon oikeasta vastaanottopisteestä. Tämä korostuu erityisesti suojaustasojen I ja II käsittelyä edellyttävien asiakirjojen osalta. Kyky käsitellä salassa pidettävää tietoa edellyttää, että henkilöstö tuntee käsittelysäännöt, omaa käsittelyoikeuden ja organisaatiolla on vaatimukset täyttävät tilat ja tietojärjestelmät. Yhteistyökumppanien osalta tulee toimeksiantoihin sisällyttää turvallisuusvaatimukset, joissa sovitaan yksityiskohtaisista menettelyistä. Salassa pidettävä tieto tulee luovuttaa jäljitettävästi ja sopimuksessa mainittujen menettelyjen mukaisesti.

6 Tietoaineistojen siirto

Tietoaineistojen siirrolla tarkoitetaan tässä yhteydessä niitä toimenpiteitä, joilla asiakirjoista otetut kopiot siirretään jakelussa määrätyille tahoille. Siirto voi tapahtua esim. postin, sähköpostin, sähköisen muistivälineen tai käsittelyoikeuksien myöntämisen avulla.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Salassa pidettävä asiakirja tulee jakaa siten, etteivät asiattomat pääse käsiksi salassa pidettävään tietoon.	kyllä	kyllä	kyllä	kyllä
(2)	Tietojärjestelmissä tietojen jakelu toteutetaan joko sähköpostin välityksellä tai tarjoamalla pääsyoikeus tietoon. Salassa pidettävän tiedon käsittelyn tulee tapahtua käyttöoikeuksien puitteissa.	kyllä	kyllä	kyllä	rajoitetusti *
(3)	Lähettäjän on varmistettava, että salassa pidettävä asiakirja luovutetaan vain sellaiselle henkilölle, jolla on tehtäviinsä liittyen siihen oikeus.	ei edellytetä	suositellaan	kyllä	kyllä
(4)	Siirrettäessä asiakirjaa sähköpostin välityksellä on varmistuttava vastaanottajan osoitteesta.	kyllä	kyllä	kyllä	sähköpostin käyttö ei sallittu
(5)	Asiakirjan siirto kuljetusyhtiön (esim posti) välityksellä Kansainvälisten asiakirjojen osalta noudatetaan lisäksi osapuolten välillä sopimuksissa määriteltyjä turvallisuusluokkakohtaisia menettelyjä.	suljetussa läpinäkymättömässä kirjekuoressa	riskianalyysin perusteella kirjattuna tai muulla turvallisella tavalla	ei sallittu; siirretään ainoastaan kuriirin tai sisäisesti oman henkilökunnan avulla	ei sallittu; siirretään ainoastaan kuriirin avulla
(6)	Salassa pidettävän turvallisuusluokitellun tiedon käsittely puhelimessa (ilman salauslaitetta)	kyllä, harkiten	ei sallittu	ei sallittu	ei sallittu
(7)	Salassa pidettävän tiedon käsittely puhelimessa (ilman salauslaitetta)	kyllä, harkiten	kyllä, harkiten	ei sallittu	ei sallittu
(8)	Salassa pidettävän tiedon käsittely salauslaitteella varustetulla puhelimella (päästä päähän salaava puhelinyhteys; salauslaitteelta edellytetään viranomaisen hyväksyntää kyseiseen suojaustasoon kuuluvan tiedon käsittelyyn)	selväkielisenä	selväkielisenä	selväkielisenä	ei sallittu
(9)	Salassa pidettävän tiedon siirto tekstiviestipalveluna	ei sallittu ilman salausta	ei sallittu ilman salausta	ei sallittu ilman vahvaa salausta	ei sallittu

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(10)	Telefax: salaamaton linjasiirto (point-to-point)	kyllä, mutta tulee varmistaa vastaanottajan läsnäolo	ei sallittu	ei sallittu	ei sallittu
(11)	Telefax: salattu linjasiirto (point-to-point) Salauslaitteelta edellytetään viranomaisen hyväksyntää.	kyllä	kyllä	kyllä	ei sallittu, paitsi toimivaltaisen viranomaisen erillispäätöksellä
(12)	Sähköisen asiakirjan siirto avoimissa tietoverkoissa	salattuna tai muutoin viranomaisen päättämällä tavalla suojattuna	salattuna tai muutoin suojattuna	ei sallittu	ei sallittu
(13)	Sähköisen asiakirjan siirto viranomaisen sisäverkoissa Salassa pidettäviä tietoaineistoja ja tietoja saa siirtää vain sellaisissa tietojärjestelmien ja tietoverkkojen osissa, jotka täyttävät kyseisen suojaustason edellyttämät vaatimukset tietovarantojen siirrolle.	selväkielisenä perustietoturvallisuustason ympäristössä	suositellaan salausta, selväkielisenä korotetun tietoturvallisuustason ympäristössä	vahvasti salattuna selväkielisenä korkean tietoturvallisuustason ympäristössä	rajoitetusti *
(14)	Sähköisen asiakirjan siirto muistivälinettä käyttäen Muistivälineet, joita käytetään kiinteän työhuoneen ulkopuolella, tulee varustaa koko tietovarannon salaavilla menetelmillä. Lisäksi luokkakohtaisesti edellytetään: (Katso myös taulukko 8, kohta 5) Sisältäessään tietoa muistivälineitä (kiintolevyt, muistivälineet) on käsiteltävä niiden sisältämän korkeimman suojaustasoa edellyttävän tiedon mukaisesti.	kyllä	kyllä	kyllä Kaikki tietojen siirto työvälineestä toiseen tulee kirjata lokiin. Samoin hävittämiset. Tiedon talletiointi on sallittu vain erikseen valvottaviin muistivälineisiin	kyllä Sallittu vain nimetyissä työasemissa. Tiedon kopiointi sallittu vain laatijan kirjallisella luvalla.

* Suojaustasoon I kuuluvia tietoja ja asiakirjoja voidaan siirtää vain erikseen nimetyissä ja hyväksytyissä korkean tietoturvallisuustason tietojärjestelmissä vahvasti salattuna tai muutoin suojattuna. Näissä järjestelmissä edellytetään, että tiedot ovat siten salattuna palvelimilla/työasemilla, että vain asiakirjan jakelun piirissä olevat saavat ne käyttöönsä.

7 Vastaanottajan toimenpiteet

Vastaanottajan toimenpiteillä tarkoitetaan niitä asioita, joita vastaanottajan tulee tehdä saadessaan käyttöönsä salassa pidettävää tietoaineistoa.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Asiakirjan vastaanottaja kirjaa vastaanotetun aineiston diaariin tai rekisteriin.	suositellaan	suositellaan	kyllä	kyllä
(2)	Vastaanoton kuittaus	ei edellytetä	tarvittaessa	kyllä	kyllä
(3)	Vastaanoton kirjaus	ei edellytetä	suositellaan	kyllä	kyllä
(4)	Asiakirjan vastaanottaja vastaa luovutuksen jälkeen kaikista asiakirjan käsittelyyn liittyvistä velvollisuuksista käsittely- ja käyttöoikeuksineen.	kyllä	kyllä	kyllä, työtehtävien hoitoon liittyen	kyllä, ei kuitenkaan oikeutta laajentaa jakelua

8 Tietoaineistojen säilytys ja tallennus

Tietoaineiston säilytyksellä ja tallennuksella tarkoitetaan niitä toimenpiteitä, joita käytetään tiedon tallentamiseen tietojen valmistelu- ja käyt-tövaiheissa.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Julkinen ja salassa pidettävä asiakirja-aineisto (tieto) tulee hallita koko elinkaaren ajan.	kyllä	kyllä	kyllä	kyllä
(2)	Käyttäjän tulee käsitellä ja huolehtia vastuullaan olevasta salassa pidettävästä tiedosta siten, että vain käyttöoikeuden omaava henkilöstö voi päästä tutustumaan siihen.	kyllä	kyllä	kyllä	kyllä
(3)	Tietoverkon palvelimille tallennettu tieto tulee olla käsittelyoikeuksilla suojattu.	kyllä	kyllä	kyllä	kyllä *
(4)	Tietoverkon palvelimille talletetun tietovarannon salaaminen tai muu vahva suojaaminen	perustietoturvallisuustason ympäristössä voidaan tallentaa selväkielisenä, suositellaan salausta	perustietoturvallisuustason palvelimilla salattuna, korotetun ja korkean tietoturvallisuustason palvelimilla sallitaan selväkielisenä	korkean ja korotetun tietoturvallisuustason palvelimilla salattuna	rajoitetusti *
(5)	Sisältäessään tietoa tietovälineitä on käsiteltävä niiden sisältämän korkeimman suojaustasoa edellyttävän tiedon mukaisesti. Laitteet tulee varustaa koko tietovarannon salaavilla menetelmillä.	suositellaan salausta	kyllä	kyllä, vahvaa salausta käyttäen	rajoitetusti *

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(6)	Käyttäjän tulee varmistua, että hänen käsittelemänsä asiakirjat tallentuvat niille tarkoitettuun ympäristöön. Tarkemmat ohjeet löytyvät sovelluskohtaisista tai organisaation antamista ohjeista. Tämä koskee kaikkia asiakirjoja.	kyllä	kyllä	kyllä	kyllä
(7)	Luonnosasiakirjoja käsitellään kuten vastaavia valmiita asiakirjoja säilytyksen ja tallennuksen osalta.	kyllä	kyllä	kyllä	kyllä
(8)	Paperimuotoiset sekä salassa pidettävää tietoa sisältävät ulkoiset muistit ja vastaavat laitteet on säilytettävä niitä varten tarkoitetuissa turvakaapeissa, holveissa tai vastaavissa lukituissa ja valvotuissa tiloissa.	suositellaan, tulee varmistaa, etteivät ulkopuoliset pääse tietoon	kyllä	kyllä	kyllä

* Suojaustasoon I kuuluvia tietoja ja asiakirjoja voidaan tallentaa vain erikseen nimetyissä ja hyväksytyissä korkean tietoturvallisuustason ympäristöissä vahvasti suojattuna. Näissä edellytetään, että tiedot ovat siten salattuna palvelimilla/työasemilla, että vain asiakirjan jakelun piirissä olevat saavat ne käyttöönsä.

9 Pääsy tietoon (tiedon käyttö)

Pääsyllä tietoon tarkoitetaan tässä yhteydessä niitä tilanteita ja menettelyjä, joilla käyttäjä saa käsittelyynsä salassa pidettävää tietoa. Tietojärjestelmissä nämä toteutetaan käyttövaltuushallinnan ja käyttäjän todentamisen keinoin.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Tietoverkon palvelimilla olevan tietovarannon lukeminen	selväkielisenä perustietoturvatason verkoista alkaen	selväkielisenä korotetun tietoturvallisuustason verkoista alkaen	selväkielisenä korkean tietoturvallisuustason verkoissa	rajoitetusti *
(2)	Etäkäyttö työnantajan tähän käyttöön antamilla välineillä ja yhteydellä edellyttäen, että käyttöympäristö täyttää tiedon suojaukselle asetetut vaatimukset	sallittu suojattua yhteyttä käyttäen	sallittu suojattua yhteyttä käyttäen, käyttäjän vahva todentaminen	sallittu vahvasti salattua tai suojattua yhteyttä käyttäen korkean tietoturvallisuustason valvotussa verkossa, käyttäjän vahva todentaminen	ei sallittu
(3)	Käyttäjän tietoverkkoon liitetyn työaseman vähimmäisvaatimukset	perustietoturvallisuustason työasema	korotetun tietoturvallisuustason työasema	korkean tietoturvallisuustason työasema	ei sallittu

* Suojaustasoon I kuuluvia tietoja ja asiakirjoja voidaan käsitellä vain erikseen nimetyissä ja hyväksytyissä korkean tietoturvallisuustason ympäristöissä vahvasti suojattuna. Näissä järjestelmissä edellytetään, että tiedot ovat siten salattuna palvelimilla/työasemilla, että vain asiakirjan jakelun piirissä olevat saavat ne käyttöönsä.

10 Tietoaineistojen arkistointi

Tietoaineistojen arkistoinnilla tarkoitetaan niitä menettelyjä, joilla varmistetaan tiedon säilyminen asetetun elinjakson ajan. Yleensä arkistot sijoitetaan käyttöympäristön ulkopuolelle.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Arkistoinnin tulee pohjautua arkistonmuodostussuunnitelmassa määriteltyihin rakenteisiin ja vaatimuksiin.	kyllä	kyllä	kyllä	kyllä
(2)	Arkistoinnissa on otettava huomioon käsittelyluokan ja sopimusten käsittelylle asettamat ehdot.	kyllä	kyllä	kyllä	kyllä
(3)	Kansainväliset asiakirjat arkistoidaan lainsäädännössä ja sopimuksissa määritellyin tavoin	kyllä	kyllä	kyllä	kyllä

11 Luokittelun päivittäminen ja poistaminen

Luokittelun päivittämisellä tarkoitetaan asiakirjan salaamistarpeen arviointia. Arvioinnissa tulee ottaa huomioon, millaisia vaikutuksia salassapidolle on arviointihetkellä. Mikäli salassapidolle ei ole enää lainmukaisia perusteita, tulee suojaustasovelvoite poistaa tai muuttaa vastaavasti.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Luokittelun uudelleen arvioinnin suorittaa asiakirjan laatinut organisaatio.	suositus	kyllä	kyllä	kyllä
(2)	Asiakirja tulee julkiseksi, kun asiakirjan laadinnasta tai vastaanottamisesta on kulunut laissa mainittu suurin salassapitoaika tai kun salassapidolle ei ole enää lainmukaisia perusteita. Asiakirjaan tehdään tästä merkintä, esimerkiksi salassapitomerkinnän yliviivaus	kyllä	kyllä	kyllä, asia tulee varmistaa laatineelta viranomaiselta	kyllä, asia tulee varmistaa laatineelta viranomaiselta
(3)	Mikäli arvioinnissa asiakirjan suojaustasoa muutetaan, tulee muutoksesta jäädä merkintä, allekirjoitus ja perustelu.	suositus	kyllä	kyllä	kyllä
(4)	Muutoksesta on tiedotettava asiakirjan ja siitä otettujen kopioiden jakelussa mainituille tahoille.	suositus	suositus	kyllä	kyllä

12 Tietoaineistojen hävittäminen

Tietoaineistojen hävittämisellä tarkoitetaan niitä toimenpiteitä, joissa tarkoituksella tuhotaan tietoaineistoja, kuten esim. asiakirjoja. Silppukoko on DIN 32757/DIN 4 mukainen.

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(1)	Alkuperäisasiakirjat tulee hävittää käyttötarpeen päätyttyä arkistonmuodostussuunnitelman mukaisesti.	kyllä	kyllä	kyllä	kyllä
(2)	Tarpeettomat asiakirjakopiot tulee hävittää käyttötarpeen päätyttyä.	kyllä	kyllä	heti	heti
(3)	Luonnosasiakirjat tulee hävittää käyttötarpeen päätyttyä.	kyllä	kyllä	heti	heti
(4)	Hävittäminen tulee suorittaa siten, etteivät salassa pidettävät ja henkilötietoja sisältävät tiedot joudu niihin oikeudettomien haltuun.	kyllä	kyllä	kyllä	kyllä
(5)	Tiedon tuottaja vastaa valmisteluvaiheessa ja organisaation käyttöön luovuttamattoman tietovarannon hävittämisestä.	kyllä	kyllä	kyllä	kyllä
(6)	Organisaation valtuuttamat henkilöt vastaavat valmiiden, viranomaisen asianhallintajärjestelmän sisältämien asiakirjojen hävittämisestä.	kyllä	kyllä	kyllä	asiakirjan allekirjoittaja vastaa *
(7)	Tiedon haltijat vastaavat heille luovutetun tietovarannon (kopiot, vastaavat tiedot) hävittämisestä.	kyllä	kyllä	ei, katso (6)	ei, katso (6)
(8)	ST I ja ST II luokkiin kuuluvat asiakirjat hävittävät valtuutetut organisaation määräämät vastuuhenkilöt. Hävittämisen yhteydessä taltioidaan asiakirjoihin tutustuneiden luettelo. Sähköisissä järjestelmissä tallennetaan käsittelytiedon sisältävät lokitiedostot (vastaavat).	-	-	kyllä	vastaava henkilö *
(9)	Arkistonhoitaja vastaa alkuperäisen asiakirjan hävittämisestä. Tilanteissa, joissa asiakirja ei siirry arkistonhoitajalle (esim. määräaikaisesti säilytettävät asiakirjat, sähköiset asiakirjat), vastaa asiakirjan haltija hävittämisestä käsittelyluokan edellyttämällä tavalla.	kyllä	kyllä	kyllä	vastaava henkilö *

Positio	Asia	SUOJAUSTASO IV	SUOJAUSTASO III	SUOJAUSTASO II	SUOJAUSTASO I
(10)	Sähköiset tiedostot tuhotaan työasemilta ja palvelimilta sekä muilta muistivälineiltä viranomaisen antamien tarkempien ohjeiden mukaisesti. Pelkkä DELETE -toiminto ei tuhoa tietoa.	kyllä	kyllä	kyllä	kyllä (asiakirjoja ei talleteta tietoverkon palvelimille)
(11)	Tietojärjestelmien käytön yhteydessä syntyvät väliaikaistiedostot on poistettava riittävän usein.	kyllä	kyllä	kyllä	kyllä
(12)	Tietoa sisältävät muistivälineet tulee hävittää viranomaisen antamien tarkempien ohjeiden mukaisesti. Muistivälineiksi luetaan kaikki laitteet, jotka taltioivat tietoa.	kyllä	kyllä	kyllä	kyllä
(13)	Tietojärjestelmissä ja tietovarannoissa oleva tieto tulee hävittää tietovarannolle määriteltyjen vaatimusten mukaisesti.	kyllä	kyllä	kyllä	kyllä (asiakirjoja ei palvelimilla)
(14)	Paperimuotoisten asiakirjojen hävittämisessä käytetään seuraavia menettelyjä:				
	1. valvotusti polttamalla	1. kyllä	1. kyllä	1. kyllä	1. kyllä
	2. silppurissa, jossa silpun koko luokittain enintään	2. 3,9 x 30 mm	2. 1,9 x 15 mm	2. 1,9 x 15 mm	2. 0,78 x 11 mm
	3. suljettuun astiaan siirrettäväksi polttolaitokseen (vast)	3. kyllä	3. sallittu, kun suljettu astia on sijoitettuna lukittuun ja valvottuun tilaan.	3. ei sallittu	3. ei sallittu

* Suojaustasoon I kuuluvien asiakirjojen hävittäminen voidaan myös määrittää organisaatiossa tiettyyn tehtävään kuuluvaksi. Tällä menettelyllä varmistetaan käytännön toimenpiteet. Asiakirjan allekirjoittajan on asiakirjaa laatiessaan/jakaessaan annettava lupa tällaiseen menettelyyn.

Liite 5. Tietoturvallisuustasojen yksityiskohtaiset vaatimukset

1 Tietoturvallisuuden hallinnan vaatimukset

1.1 Johtajuudelle asetettavat vaatimukset

Osa-alueen nimi	1.1.1 Strateginen ohjaus
Tavoitteet	Organisaatio on tunnistanut ydintoimintoihinsa liittyvät jatkuvuuden ja erityistilanteiden hallintaa sekä tiedon turvaamista ohjaavat tekijät ja velvoitteet. Toiminnan jatkuvuuden hallinnan ja tiedon turvaamisen toimenpiteet tukevat organisaation ydintoiminnan tavoitteita.
Perustason vaatimukset	1. Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu. 2. Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu. 3. Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.
Korotetun tason lisävaatimukset	4. Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.
Korkean tason lisävaatimukset	5. Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma. 6. Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia.
Esimerkkejä hyvistä käytännöistä	• Vaatimuksiin 3 ja 4: Organisaatiolla on tietoturvapolitiikka ja siitä johdettu tietoturvastrategia, joka kuvaa miten politiikan päämäärään päästään.
Apuvälineitä ja malleja	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007) • Erityisesti liite 1: Mallipolitiikat ja suunnitelmarungot Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006) Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004) Valtioneuvoston periaatepäätös tietoturvallisuudesta valtionhallinnossa 2009 sekä tausta-aineisto CAF-arviointimalli www.vm.fi/caf
Huomioita	Kaikki lähtee siitä, että organisaation johto on sitoutunut tietoturvallisuuteen ja osaa tulkita ydintoimintojen vaatimukset tietoturvallisuuden ohjaukseksi.

Osa-alueen nimi	1.1.2 Resursointi ja organisointi
Tavoitteet	Jatkuvuuden hallinnalle ja tiedon turvaamiselle on asetettu tavoitteisiin nähden riittävät resurssit.
Perustason vaatimukset	1. Organisaatioon on nimitetty tietoturvavastaava, jonka työnkuvassa on mainittu tietoturvavastuut. 2. Tietoturvavastaavalla on aikaa tietoturvavastuidensa suorittamiseen.
Korotetun tason lisävaatimukset	3. Kaikkien tietoturvavastuita omaavien työnkuvissa vastuu on mainittu. 4. Organisaatiossa on sen kokoon ja tavoitteisiin nähden riittävästi tietoturvahenkilöstöä. 5. Tietoturvallisuuden resursointi on huomioitu organisaation toiminta- ja taloussuunnittelussa tai budjetissa ja toteutumista seurataan.
Korkean tason lisävaatimukset	6. Tietoturvavastaava on päätoiminen.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Organisaation tietoturvavastaavana toimii hallintopäällikkö, joka hoitaa tietoturva-asioita oman päätoimensa ohella. • Vaatimukseen 3: Organisaatiossa ei käytetä henkilökohtaisia työnkuvia, vaan roolikuvauksia. Asiointijärjestelmän pääkäyttäjän roolikuvauksessa mainitaan vastuu käyttöoikeuksien poistamisesta pyyntöjen mukaan. • Vaatimukseen 4 ja 5: Organisaatiolle tulee uusia tehtäviä, jotka vaativat sen siirtymistä korkealle tietoturvallisuustasolle vuonna 2012. Tämän vuoksi tietoturvatyöhön on panostettava lisää, mikä kirjataan budjettiin.
Apuvälineitä ja malleja	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007) • Tietoturvallisuuden esimerkkivuosikello, s. 31 • Liite 2: Tietoturvavastuut rooleittain
Huomioita	Pienessäkin organisaatiossa voidaan vähillä resursseilla päästä perustasolle. Jos tarvitaan korkeampaa tietoturvallisuustasoa, resurssien tulee kasvaa.

Osa-alueen nimi	1.1.3 Yhteistyön koordinointi
Tavoitteet	Jatkuvuuden hallinnan ja tiedon turvaamisen suunnittelu toteutetaan ydin- ja tukitoimintojen yhteistyönä.
Perustason vaatimukset	1. Organisaation johto ja tietoturvallisuuden eri osa-alueiden vastuuhenkilöt keskustelevat säännöllisesti. 2. Organisaatiossa on säännöllisesti kokoontuva tietoturva-asioita käsittelevä yhteistyöryhmä.
Korotetun tason lisävaatimukset	3. Johdon tapaamiset ovat vähintään kerran vuodessa. 4. Tietoturva-asioita käsittelevä yhteistyöryhmä kokoontuu vähintään kaksi kertaa vuodessa.
Korkean tason lisävaatimukset	5. Tapaamisissa käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia. 6. Tapaamisista pidetään pöytäkirjaa ja sovittujen toimenpiteiden toteutumista seurataan.
Esimerkkejä hyvistä käytännöistä	• Vaatimuksiin 1, 3, 5: ISO27001-standardin mukaista tietoturvallisuuden hallintamallia noudattava organisaatio järjestää puolivuosittain johdon katselmointitilaisuuden. • Vaatimukseen 1: Viraston tietoturvapäällikkö tapaa viraston ylintä johtoa kerran kuukaudessa. Myös viraston aluetoimipisteen tietoturvavastaava tapaa aluetoimipisteen paikallista johtoa säännöllisesti kuukausipalaverissa. • Vaatimukseen 2 ja 4: Organisaatiossa on kaikkia turvallisuusasioita käsittelevä kuukausittain kokoontuva ryhmä. • Vaatimukseen 2: Pienen organisaation johtoryhmä käsittelee tietoturva-asioita vähintään kerran vuodessa ja tietoturvavastaava osallistuu käsittelyyn.
Apuvälineitä ja malleja	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) • luku 2
Huomioita	Tavoitteena on se, että tietoturvavastaavat ja organisaation ylin johto keskustelevat säännöllisesti keskenään. Yhteistyötä on hyvä tehdä muillakin organisaatiohierarkian tasoilla ja muistakin turvallisuuden osa-alueista vastaavien kanssa, mutta näissä vaatimuksissa keskitytään siihen, että ylin johto voi ohjata tietoturvatyötä.

Osa-alueen nimi	1.1.4. Raportointi ja viestintä sidosryhmille
Tavoitteet	Viestinnän ja raportoinnin vastuut ja toimintamalli sidosryhmien kanssa on määritetty siten, että osapuolilla on toimintaan, sen kehittämiseen ja päätöksentekoon tarvittavat tiedot.
Perustason vaatimukset	1. Sidosryhmät, joille organisaatio on vastuussa tietoturvallisuudesta, ja niiden kontaktipisteet on tunnistettu. 2. Johto on organisoinut ja vastuuttanut sidosryhmiin vaikuttavista tietoturva-asioista raportoinnin sekä tietoturvapoikkeamista tiedottamisen.
Korotetun tason lisävaatimukset	3. Sidosryhmille raportoidaan tietoturvallisuudesta vuosittain tai johdon määrittelemällä tavalla. 4. Sidosryhmäraportilla on mallipohja.
Korkean tason lisävaatimukset	5. Jos muuta ei sovita, raportin sisältöön kuuluu mittaustietoa vaatimuksenmukaisuudesta, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset. 6. Raportointia kehitetään sidosryhmien palautteen perusteella.
Esimerkkejä hyvistä käytännöistä	• Vaatimukset 1 ja 3: Palvelukeskus on vastuussa palveluiden tilaajilleen palveluidensa tietoturvallisuudesta ja osana palvelua muodostuu neljännesvuosittainen raportti, jossa on tietoturvaosio. • Vaatimukseen 2: Kansalaisten henkilötietoja käsittelevällä organisaatiolla on olemassa malli siitä, miten näiden tietojen vuotamisesta tiedotetaan sidosryhmille, mm. kansalaisille.
Apuvälineitä ja malleja	Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006) • Luku 5.6: Esimerkki raportointimenettelyistä ja raportin sisällöstä Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005) • Luku 2.2.6: Poikkeamatilanteen viestintäsuunnitelman luonti
Huomioita	Osion tarkoitus on saada organisaatiot tunnistamaan tahot, joille tietoturvallisuudesta tulisi raportoida, vaikka taho ei itse ole vielä herännyt vaatimaan tietoa. Tämä edistää koko valtionhallinnon tietoturvallisuutta.

Osa-alueen nimi	1.1.5 Johtaminen erityistilanteessa
Tavoitteet	Erityistilanteiden hallinta on organisoitu ja huomioitu toimintamalleissa.
Perustason vaatimukset	1. Tietoturvapoikkeamien käsittely on organisoitu ja vastuutettu. 2. Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.
Korotetun tason lisävaatimukset	3. Organisaatiossa on kirjallinen malli tietoturvapoikkeamien käsittelyyn. Ohjeessa on määritelty roolitasolla kuka selvittää tapahtunutta kenen määräyksestä ja kuka päättää viranomaiskontakteista (esim. esitutkintapyynnön teosta) ja tiedottamisesta. 4. Tietoturvapoikkeamista tehdään jälkikäteisanalyysi ja käynnistetään tarvittavat korjaavat toimenpiteet tapahtuman uusiutumisen ehkäisemiseksi.
Korkean tason lisävaatimukset	5. Havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto. 6. Tietoturvapoikkeamista vaihdetaan tietoja kumppanien kanssa ja kumppanien kokemuksia käytetään hyväksi.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 5: Tietoturvapoikkeamista tehdään vuosittainen trendianalyysi ongelman syyn mukaisesti jaoteltuna. • Vaatimukseen 6: Yhteistyötä toteutetaan benchmark-arviointien yhteydessä.
Apuvälineitä ja malleja	Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005) • Luku 2.2.4: Reagoinnin organisointi ja toimivaltuudet ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009)
Huomioita	Tietoturvapoikkeama on VAHTIn määritelmän mukaan tahallinen tai tahaton olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palveluiden eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyys on tai saattaa olla vaarantunut.

Osa-alueen nimi	1.1.6 Raportointi johdolle
Tavoitteet	Tiedot kehittämistoimenpiteiden toteutumisesta ja kustannuksista välittyvät organisaation johdolle.
Perustason vaatimukset	1. Tietoturvallisuudesta raportointi on vastuutettu ja organisoitu. 2. Tietoturva-asioista raportoidaan organisaation johdolle säännöllisesti.
Korotetun tason lisävaatimukset	3. Raportointimenettely on kuvattu kirjallisesti. 4. Tietoturva-asioista raportoidaan organisaation johdolle vähintään vuosittain.
Korkean tason lisävaatimukset	5. Jatkuva raportointi perustuu päätettyihin toiminnan mittareihin. 6. Raportin sisältöön kuuluu mittaustietoa resurssien käytöstä, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1 ja 3: Organisaatiossa on olemassa johdon hyväksymä vuosittaisen tietoturvaraportin pohja. Raportin luominen on tietoturvapäällikön vastuulla.
Apuvälineitä ja malleja	Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006) • Luku 5.6: Esimerkki raportointimenettelyistä ja raportin sisällöstä
Huomioita	Johto on vastuussa organisaation toiminnasta. Jotta johto voi tehdä perusteltuja päätöksiä tarvittavista riskienhallintatoimenpiteistä, sen on saatava tietoa jo tehtyjen toimien riittävyydestä ja vaikutuksista sekä mahdollisista ongelmakohdista.

1.2 Toiminnan suunnittelulle asetettavat vaatimukset

Osa-alueen nimi	1.2.1 Toimintaympäristön vaikutus
Tavoitteet	Toimintaympäristö ja sen vaikutus toimintaan tunnetaan.
Perustason vaatimukset	1. Erilliset tietojen käsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät ja toiminnot on tunnistettu. 2. Kunkin toimintaympäristön erityisvaatimukset ja tavoitteet tietoturvallisuuden osalta on tunnistettu.
Korotetun tason lisävaatimukset	3. Toimintaympäristöt ja niihin kuuluvat järjestelmät on dokumentoitu. 4. Ympäristö- ja järjestelmälistaukset katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain
Korkean tason lisävaatimukset	5. Ympäristöjen elinkaaren vaiheet on dokumentoitu ja dokumentissa on kriteerit milloin ja miten ympäristö siirtyy vaiheesta toiseen. 6. Kunkin elinkaaren vaiheen erityisvaatimukset tietoturvallisuuden osalta on määritelty ja dokumentoitu.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Organisaatiolla on päätoimipaikka ja alueellinen yksikkö. Alueellinen yksikkö käsittelee lupa-asioita, muut toiminnot tapahtuvat päätoimipaikassa. Lupa-asioihin liittyvät tietojärjestelmät on myös sijoitettu alueellisen yksikön tiloihin. • Vaatimuksiin 1 ja 2: Organisaatiossa on samasta organisaation toiminnalle kriittisestä tietojärjestelmästä kolme erillistä ympäristöä: kehitys-, testi- sekä tuotantoympäristöt, joilla kullakin on erillinen käyttäjätunnusten hallintapolitiikka. • Vaatimukseen 5: Organisaatio vaihtaa sähköpostijärjestelmänsä toiseen ja siirtymäaikana sähköpostijärjestelmiä on kaksi, vanha ja uusi. Vanha järjestelmä on elinkaarensa käytöstäpoistamisvaiheessa, uusi tuotantokäytössä. • Vaatimukseen 6: Organisaatiossa on tehty päätös, että testivaiheessa olevassa tietojärjestelmässä testiaineistojen henkilötiedot sotketaan.
Apuvälineitä ja malleja	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) • luku 1.3 ITIL ja ISO/IEC20000.
Huomioita	On tärkeää tunnistaa oman toimintaympäristön yhtenäisyys tai hajanaisuus, olipa kyse esimerkiksi toimitiloista, etätyöpisteistä tai tietovarannoista. Organisaation toimintaympäristö vaikuttaa riskianalyysin kautta moneen tietoturvallisuuden osa-alueeseen ja se on erityisen tärkeä myös jatkuvuus- ja toipumissuunnittelun kannalta. Ympäristöjä listattaessa on tärkeää ymmärtää paitsi fyysinen erillisyys, myös ajallinen elinkaari.

Osa-alueen nimi	1.2.2 Tavoitteiden määrittely
Tavoitteet	Ydintoiminnasta on johdettu sen edellyttämien palvelujen jatkuvuuden hallinnan, erityistilanteiden ja tiedon turvaamisen vaatimukset.
Perustason vaatimukset	1. Kunkin ydintoiminnon ja -prosessin tietoturvallisuuden kannalta suojattavat kohteet on tunnistettu ja luokiteltu vaadittavan tietoturvallisuuden tason mukaisesti. 2. Ydintoimintojen tai -prosessien tavoitteisiin on liitetty myös tietoturvatavoitteita.
Korotetun tason lisävaatimukset	3. Tietoturvatavoitteiden määrittelyssä on otettu huomioon sekä luottamuksellisuus, eheys että saatavuus. 4. Ydintoiminnoista ja -prosesseista on karkean tason toiminto- tai prosessikuvaukset.
Korkean tason lisävaatimukset	5. Toiminto- tai prosessikuvauksiin on liitetty tietoturvallisuuden kannalta oleelliset tietoturvaprosessit tai toimet tai ne on dokumentoitu erikseen. 6. Toimintojen tietoturvatavoitteisiin on liitetty suoriutumista kuvaavia mittareita.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Tukikäsittelyprosessille on määritelty suojattaviksi kohteiksi tuen hakijoista koostettu henkilörekisteri, päätöstietojärjestelmä sekä sähköisen asioinnin mahdollistava tietojärjestelmä, jotka on luokiteltu niiden sisältämän tiedon luottamuksellisuuden mukaan. • Vaatimukseen 2: Toimintojen tietoturvatavoitteet on määritelty toimintojen omissa tuloskorteissa. • Vaatimuksiin 3 ja 6: Asiointitoiminnon sähköiselle palvelulle on määritelty tietoturvatavoitteeksi, että sen tulee olla kansalaisten käytettävissä 99,9% virka-ajasta ja että sellaisten tietoturvapoikkeamien määrä, jossa kansalaiset pystyvät näkemään tai muuttamaan toistensa tietoja palvelua käyttäessään, on vuositasolla nolla. • Vaatimukseen 5: Organisaation yksi ydintoiminto on asiointiprosessi. Prosessiin on kuvattu, miten asioijan henkilöllisyys tarkistetaan, miten asiointitietoja säilytetään ja miten tiedot suojataan jos tietoja siirretään toisille viranomaisille.
Apuvälineitä ja malleja	Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006) • Luku 3: Tietoturvallisuuden tulosohjaus • Luku 4.4: Tietoturvatoiminnan mittarit Prosessien kuvaus (JHS 152) • Liite 1: Prosessin perustietolomake • Liite 2: Toiminnot-taulukko
Huomioita	Tietoturvallisuuden tavoitteet määritellään ydintoimintojen näkökulmasta. Ydintoimintojen suojattavien kohteiden (eli tietoaineistojen, tietojärjestelmien, rekisterien jne.) määrittely ja kohteiden tietoturvavaatimukset ovat merkittävä taustatekijä tietoturvatavoitteiden asettamisessa. Osa suojattavista kohteista on koko organisaatiolle yhteisiä (esim. työasemat, tietoliikenne), mutta niidenkin tärkeys eri avainprosessien toiminnalle vaihtelee. Kun tavoitteet ovat selvillä, tehdään riskien arviointi, jotta selvitetään mitä riskejä tavoitteiden toteutumiseksi tässä toimintaympäristössä on.

Osa-alueen nimi	1.2.3 Toiminnan kehittäminen riskien arvioinnilla
Tavoitteet	Organisaatio varmistaa, että tietoturvallisuuden taso vastaa organisaation strategisia tavoitteita. Tietoturvallisuuden kehittäminen ottaa huomioon organisaatiota kohtaavat tietoturvauhat ja riskit. Säännöllinen riskienhallintamenettely on käytössä.
Perustason vaatimukset	1. Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia. 2. Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä.
Korotetun tason lisävaatimukset	3. Organisaatiossa tehdään ydintoimintojen tietoturvariskien arviointia vähintään vuosittain. 4. Organisaatiolla on riskien arvioinnin menetelmä ja ohjeistus. 5. Organisaatiolla on kirjallinen tietoturvasuunnitelma, joka määrittelee mitä teknisiä ja hallinnollisia toimia ja prosesseja organisaatiossa käytetään havaittujen tietoturvariskien hallitsemiseksi.
Korkean tason lisävaatimukset	6. Organisaatiossa tehdään tietoturvariskien arviointia myös suurten muutosten yhteydessä. 7. Organisaatiolla on riskienhallintapolitiikka. 8. Suurimmista riskeistä pidetään koko organisaation tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan.
Esimerkkejä hyvistä käytännöistä	• Vaatimuksiin 1 ja 4: Organisaatiossa on sovittu, että tietoturvariskien arviointia tehdään kahdessa osassa. Ensin ydintoimintojen vastuuhenkilöt pitävät toiminnon oman tietoturvariskien arvioinnin ja tämän jälkeen on organisaation yhteinen tietoturvariskien arviointitilaisuus, jossa käsitellään yhteisiä asioita ja toimintojen arviointitilaisuuksissa esille tulleita riskejä. • Vaatimuksiin 2 ja 4: Riskien arvioinnissa erittäin suureksi riskiksi organisaatiossa arvioitiin vahingossa tapahtuva ei-julkisen materiaalin tietovuoto kannettavien tietovälineiden kautta. Päätettiin investoida helppokäyttöiseen salausohjelmistoon ja henkilöstön koulutukseen riskin vähentämiseksi halutulle tasolle. Tietoturvasuunnitelmaa päivitettiin tämän johdosta.
Apuvälineitä ja malleja	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa VAHTI 7/2003 • Luku 3.2: Riskienarvioinnin malliprosessi • Taulukko 5, s 47 – esimerkki riskien hallintasuunnitelmasta • Liite 2: Tietoriskien tunnistamisen tarkistuslistoja Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007) • Tietoturvasuunnitelman runko, s. 88 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) • luku 6 ENISA, riskienhallintamenetelmien tietoportaali (englanninkielinen)
Huomioita	Riskianalyysi tehdään vasta kun toimintaympäristö ja ydintoimintojen asettamat tavoitteet toiminnalle ovat tiedossa. Riskianalyysin perusteella suunnitellaan tarvittavat tekniset suojaustoimet ja tietoturvallisuuden hallintaprosessit, jotta tietoturvallisuudelle asetetut tavoitteet saavutettaisiin ja riskit pysyisivät hyväksyttävällä tasolla tässä toimintaympäristössä. Valitut toimenpiteet ja periaatteet kuvataan tai päivitetään tietoturvasuunnitelmaan tai muuhun vastaavaan dokumenttiin.

Osa-alueen nimi	1.2.4 Toimintaverkoston hallinta
Tavoitteet	Palvelujen jatkuvuus ja tiedon turvaaminen kumppaniverkostossa on suunniteltu ja sovittu.
Perustason vaatimukset	1. Organisaatiossa on tiedossa, missä toimintaverkostoissa organisaatio on mukana sekä mitä alihankkijoita ja yhteistyökumppaneita sen tietojen kanssa toimii missäkin roolissa.
Korotetun tason lisävaatimukset	2. Organisaatiolla on kirjallinen dokumentti, jossa kuvataan sen osallistumista ja roolia erilaisissa alihankinta- ja yhteistyöverkostoissa sekä osallistumisen yleisiä tietoturvavaatimuksia.
Korkean tason lisävaatimukset	3. Toimintoverkostot on luokiteltu tietoturvallisuustason mukaan ja kullakin luokalla on omat tietoturvavaatimuksensa. 4. Palveluntarjoajaksi voidaan valita vain sellainen palveluntarjoaja, jolla on mahdollisuus suojata asiakirjojen luottamuksellisuus ja tarvittaessa selvittää luottamuksellisuuden loukkaukset sähköisen viestinnän tietosuojalain (516/2004) 13 a - 13k §.ssä tarkoitetulla tavalla.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Toimenkuvien määrittelyn yhteydessä on sovittu, että hankinnoista vastaavat pitävät yllä toimintaverkoston tilannekuvaa alihankkijoiden osalta. • Vaatimukseen 2: Tietohallintostrategiassa mainitaan, että ICT- tukitoimintoja ulkoistettaessa edellytetään alihankkijoilta ja yhteistyökumppaneilta vähintään samaa tietoturvallisuustasoa kuin organisaatiolta itseltään. • Vaatimukseen 2: Palvelukeskus pitää rekisteriä kunkin asiakasorganisaation tilaamista palveluista ja niiltä edellytetyistä tietoturvallisuustasoista.
Apuvälineitä ja malleja	Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi (VAHTI 7/2006) ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) • luku 5
Huomioita	Tässä osiossa olennaista on se, että organisaatio tiedostaa, missä alihankintaketjuissa ja muissa yhteistyöverkostoissa se on mukana ja mitä se tarkoittaa verkostoissa käsiteltävien tietojen kannalta. Toimintaverkostot voidaan selvittää joko keskitetysti tai hajautetusti sen mukaan ovatko hankinnat tai yhteistyöpäätökset yleisesti keskitettyjä vai hajautettuja.

Osa-alueen nimi	1.2.5 Erityistilanteiden hallinta
Tavoitteet	Erityistilanteiden hallinnan menettelyt on suunniteltu, koulutettu ja harjoiteltu.
Suomen erityis-vaateet	1. Organisaation johto on tiedostanut mitä yhteiskunnan elintärkeiden toimintojen turvaamiseen (YETT) liittyviä vastuita organisaatiolla on.
Perustason vaatimukset	2. Organisaatiolla on jatkuvuussuunnitelma tai -suunnitelmia.
Korotetun tason lisävaatimukset	3. Jatkuvuussuunnitelmien päivitys ja katselmointi on vastuutettu ja organisoitu. 4. Jatkuvuussuunnitelmien toimivuutta testataan, harjoitellaan ja arvioidaan säännöllisesti.
Korkean tason lisävaatimukset	5. Jatkuvuussuunnitelmien toimivuutta harjoitellaan keskeisten yhteistyökumppanien kanssa.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 2: Eri jatkuvuussuunnitelmia testataan vuorovuosin pöytätestinä tai tarkistuslistatestinä. • Vaatimukseen 4: Organisaatiossa järjestetään suunnitelmien testausta vuosittain jotakin jatkuvuutta uhkaavaa tilannetta simuloiden.
Apuvälineitä ja malleja	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007) • Jatkuvuussuunnitelman runko s. 90 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) Huoltovarmuuskeskuksen suositukset Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, VN periaatepäätös 2006 • Luku 3.3: Ministeriöiden strategiset tehtävät toimintojen turvaamiseksi • Liite 2: Varautuminen erityistilanteisiin
Huomioita	Jatkuvuudella tarkoitetaan organisaation toimintojen jatkuvuutta erilaisissa häiriötilanteissa. Suunnitelmat ICT-järjestelmien teknisestä palautumisesta erilaisista häiriöistä käsitellään liitteessä 2 nimellä Toipumissuunnittelu. Yhteiskunnan elintärkeiden toimintojen varautumiseen ja huoltovarmuuteen liittyvien vaatimusten työ on kesken (VARE, HUOVI) ja ne tullaan määrittelemään erikseen.

1.3 Henkilöstölle asetettavat vaatimukset

Osa-alueen nimi	1.3.1 Osaamisen ja tietoisuuden kehittäminen sekä sanktiot
Tavoitteet	Jatkuvuuden hallinnan ja tiedon turvaamisen osaamiselle on asetettu rooli- tai tehtäväkohtaiset vaatimukset, osaamistaso tunnetaan ja osaamista kehitetään. Organisaatio kannustaa henkilöstöä noudattamaan ja kehittämään hyvää jatkuvuuden hallinnan ja tiedon turvaamisen toimintamallia. Organisaatiossa on sovittu tapa toimia turvallisuuspoikkeamissa ja väärinkäytöstilanteissa.
Suomen erityisvaateet	1. Työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§).
Perustason vaatimukset	2. Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään. 3. Perehdyttämistilanteessa käsitellään myös tietoturva-asioita. 4. Muuttuneista tietoturvaohjeista ja -käytännöistä tiedotetaan kaikille organisaatiossa toimiville. 5. Sääntöjen noudattamista seurataan ja poikkeamiin puututaan.
Korotetun tason lisävaatimukset	6. Organisaatiossa on kirjallinen tietoturvallisuuden koulutussuunnitelma. 7. Perehdyttäjällä on kirjallinen lista käsiteltävistä tietoturva-asioista. 8. Henkilöstön osallistumista koulutuksiin seurataan. 9. Tietoturvamääräysten ja -ohjeiden rikkomisen seuraukset on kuvattu organisaatiossa ja tiedotettu kaikille organisaatiossa työskenteleville. 10. Esimies ja alainen käyvät vuosittain keskustelun työn tietoturvavastuista ja osaamisen kehittämisen tarpeista. 11. Henkilöstön tietoturvaosaamisesta varmistutaan
Korkean tason lisävaatimukset	12. Tietoturvakoulutuksessa otetaan huomioon organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat. 13. Hyvistä tietoturvateoista annetaan positiivista huomiota.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 2: Organisaatiossa järjestetään vuosittain tietoturvakoulutus henkilöstölle sekä erillinen tietoturvakoulutus alihankkijoille. Tietoturvavastaava käy alan seminaareissa. • Vaatimuksiin 2 ja 9: Tietoturvapolitiikassa lukee, mitä seurauksia tietoturvaohjeiden ja määräysten noudattamatta jättämisestä voi seurata. Käytännön koulutuksessa on mainittu myös, mistä asioista ei saa puhua organisaation ulkopuolella. • Vaatimukseen 8: Tietoturvakoulutuksessa kerätään osallistujien nimilista ja koulutettujen määrää seurataan vuosittain. • Vaatimukseen 8: Organisaatiossa käytetään tietoturvakoulutukseen tietokoneavusteista -koulutuspakettia, joka pitää kirjaa koulutuksen läpikäyneistä ja muistuttaa vielä kouluttamattomia kurssista. • Vaatimukseen 11: Henkilöstölle tehdään säännöllisesti tietoturvakysely, jossa selvitetään, onko koulutus lisännyt ymmärrystä tai tietoisuutta. • Vaatimukseen 13: Johto tai tietoturvapäällikkö kehuu julkisesti henkilöitä tai ryhmiä hyvästä tietoturvallisuuden huomioon ottamisesta.
Apuvälineitä ja malleja	Henkilöstön tietoturvaohje (VAHTI 10/2006) • Koulutusmateriaali (Powerpoint) Tietoturvakouluttajan opas (VAHTI 11/2006) ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) • luku 4 ENISA tietoturvatietoisuusohje • Liitteet 1-4, Tietoturvatietoisuusprojektin suunnittelupohjia • Liite 5: Kansalaisten tietoturvatietoisuuskyselyn pohja Tietoturvakoulu
Huomioita	Henkilöstön tietoturvatietoisuus sekä positiivinen asenne tietoturvallisuutta kohtaan on avainasemassa henkilöstön tietämättömyydestä johtuvien tietoturvapoikkeamien estämisessä. Koska tietoturvallisuus voidaan mieltää negatiivisena ja jopa työtä haittaavana asiana, positiivisen palautteen vaikutusta ei kannata aliarvioida.

Osa-alueen nimi	1.3.2 Henkilöresurssien ja tehtävien hallinta
Tavoitteet	Henkilöstö ja sen käyttö on suunniteltu ja mitoitettu ydintoimintojen jatkuvuuden hallinnan ja tiedon turvaamisen edellyttämällä tavalla. Avainroolit ja -henkilöt on tunnistettu ja varajärjestelyt on suunniteltu.
Perustason vaatimukset	1. Toteutettavaksi valitut tietoturvatoimenpiteet ja -prosessit on organisoitu ja vastuutettu. 2. Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai -henkilöt.
Korotetun tason lisävaatimukset	3. Toteutettavaksi valituista tietoturvaprosesseista tai -toimenpiteistä ja niiden vastuuhenkilöistä on luettelo. 4. Tietoturvallisuuden varahenkilöt on koulutettu tehtäväänsä.
Korkean tason lisävaatimukset	5. Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu. 6. Organisaatiossa on tehty tietoturvallisuuden osaamiskartoitus.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Palomuurin ylläpito on havaittu tarpeelliseksi tietoturvaprosessiksi, ja sille on määritelty omistaja ja käytännön toteuttajat. Käytännön toteuttajaksi on valittu ulkoistuskumppani. • Vaatimukseen 2: Tietoturvapäällikkö on todettu organisaatiossa avainrooliksi ja hänelle on nimetty varahenkilö. Tietoturvapäällikön kanssa asioidaan sähköpostitse rooliosoitteen tietoturvapaallikko@virasto.fi kautta ja varahenkilöllä on pääsy tähän sähköpostilaatikkoon, jotta hän on selvillä vireillä olevista toimista.
Apuvälineitä ja malleja	Tärkein tekijä on ihminen, henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008) • Luku 4.6.2: Turvallisuusselvitykset • Liite 4: Virastojen hakeutuminen turvallisuusselvitysmenettelyyn ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009) • luku 4
Huomioita	Toteutettavaksi valitut tietoturvatoimenpiteet ja -prosessit voivat tulla useaa kautta. Tyypillisesti uusia toteutettavia tietoturvatoimia tai -prosesseja syntyy ylempänä käsitellyn ”Toiminnan kehittäminen riskien arvioinnin kautta” sekä jäljempänä käsitellystä ”Toiminnan arviointi ja todentaminen” -osioiden tuloksina. Ne on hyvä dokumentoida tietoturvasuunnitelmaan tai vastaavaan Tietojärjestelmiin liittyviä tietoturvaprosesseja on käsitelty liitteessä 2..

Osa-alueen nimi	1.3.3 Erityistilanteissa toimiminen
Tavoitteet	Kriittisten toimintojen häiriöiden hallintaohjeet on laadittu, koulutettu ja toiminta harjoiteltu.
Suomen erityisvaateet	1. Sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös tietoturvapoikkeamatilanteita selvitettäessä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§ sekä Laki yksityisyyden suojasta työelämässä 6. luku).
Perustason vaatimukset	2. Henkilöstö tietää, kenelle tietoturvapoikkeamista ja -tapauksista tai niiden uhkista tulee ilmoittaa.
Korotetun tason lisävaatimukset	3. Tietoturvapoikkeamia selvittävät henkilöt on koulutettu tehtäväänsä.
Korkean tason lisävaatimukset	4. Organisaatiossa on tietoturvapoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Organisaatiossa on Laki yksityisyyden suojasta työelämässä 6. luvun huomioon ottava kirjallinen sähköpostipolitiikka.
Apuvälineitä ja malleja	Viestintäviraston CERT-FI:n ohjeita Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005 Valtionhallinnon sähköpostin käsittelyohje, VAHTI 2/2005 • Liite 2: Sähköpostin käsittelysäännöt • Liite 5: Malli sähköpostilaatikon avauslomakkeeseen
Huomioita	Erityistilanteiden selvityksen vastuutus ja organisointi kuuluu ylempänä johdon osuudessa käsiteltyyn ”Johtaminen erityistilanteissa” -osioon. ICT-järjestelmien lokienhallintaa käsitellään liitteen 2 osassa "Tietoturvapoikkeamien valvonta" Organisaation toiminnan jatkuvuuden varmistamista käsitellään ylempänä ”Erityistilanteiden hallinta” -osiossa. ICT-järjestelmien toipumissuunnittelu käsitellään liitteen 2 osassa ”Tietojärjestelmien toipuminen häiriöistä”..

1.4 Kumppanuuksille ja resurssien hallinnalle asetettavat vaatimukset

Osa-alueen nimi	1.4.1 Sopimusten hallinta
Tavoitteet	Sopimuksissa kirjataan liiketoiminnan jatkuvuuden hallinnan, erityistilanteiden hallinnan ja tiedon turvaamisen vaatimukset sekä niiden toteuttaminen. Kriittisen toiminnan jatkuvuuden ja tiedon turvaamisen hallintavelvoite on ulotettu koko toimitta-javerkostoon.
Perustason vaatimukset	1. Kumppanuus- ja hankintatoiminta on vastuutettu ja organisoitu. 2. Kumppanin kanssa tehdään kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.
Korotetun tason lisävaatimukset	3. Kumppanille asetetaan tarvittavat tietoturvavaatimukset jo tarjouspyyntö- tai kumppanuus-neuvotteluvaiheessa. 4. Kumppanuussopimuksessa määritellään mitä tietoturvallisuustasoa kumppanin ja mahdollisen kumppanin alihankintaverkoston on kohteen luonteen huomioon ottaen noudatettava.
Korkean tason lisävaatimukset	5. Ennen sopimuksen solmimista organisaatio auditoi tai pyytää kirjallisen selvityksen kumppanin yhteistyön kohteeseen liittyvistä tietoturvamenettelyistä. 6. Sopimuksessa on määritelty sanktiot tietoturvapoikkeamista ja -loukkauksista.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 2: Sopimuksia laadittaessa käytetään vakiomuotoista turvallisuusliitettä joka kattaa myös tietoturva-asiat. • Vaatimukseen 2: Valitulla kumppanilla on puitesopimus koko hallinnonalan kanssa. Jos puite-sopimuksessa on jo riittävät tietoturvavaatimukset hankinnan kohteeseen nähden, uutta tieto-turvasopimusta ei tarvitse tehdä. • Vaatimukseen 3: Jo tarjouspyyntövaiheessa otetaan huomioon hankinnan kohteen tietoturva-tarpeet tekemällä kohteeseen riskianalyysi ja sen pohjalta tarjouspyyntöön tietoturvavaati-mukset. • Vaatimukseen 4: Perustason virasto ulkoistaa tietojärjestelmän ylläpidon ulkoiselle organisaa-tiolle. Tietojärjestelmässä käsitellään henkilötietoja, joten tietojärjestelmää ylläpitävän palve-luntarjoajan tulee täyttää tämän dokumenttikokoelman korkean tason vaatimukset.
Apuvälineitä ja malleja	Tärkein tekijä on ihminen, henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008) • Luku 4.7 Kansainvälinen henkilöturvallisuustodistus • Luku 4.10 Ostopalvelujen turvallisuus Julkisen hallinnon IT-hankintojen sopimusehdot JIT 2007 (JHS 166) • Yleiset ehdot, luku 27 • Sovellushankinnan mallisopimus, luku 10 • Palveluiden mallisopimus, luvut 7 ja 11 • Konsultoinnin mallisopimus, luku 8 Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi (VAHTI 7/2006) • Liitteet 1A ja 1B: Turvallisuussopimusmalleja • Liite 5: Henkilötietojen käsittelyn tarkistuslista • Liite 6: Kumppanin tietoturvamenettelyiden tarkistuslista Huoltovarmuuskeskuksen Sopimuksiin perustuva varautuminen – hankkeen Sopiva-vaatimukset
Huomioita	Mitä lähempänä sopimuksen kohde on organisaation ydintoimintaa, sitä paremmin tietoturvavaa-timukset tarjouspyyntöihin tai sopimuksiin voidaan johtaa aikaisemmin käsitellyistä ”Tavoitteiden määrittely” sekä ”Toiminnan kehittäminen riskien arvioinnilla” -osioiden tuloksista. JIT 2007 -mallisopimuksissa tietoturvallisuus on otettu huomioon varsin yleisellä tasolla. Niitä käy-tettäessä kustakin hankinnan kohteesta on syytä tehdä erillinen tietoturvaliite ja vaatia mm. audi-tointimahdollisuus.

Osa-alueen nimi	1.4.2 Toiminnan varmistaminen erityistilanteessa
Tavoitteet	Kumppanin häiriöiden ja erityistilanteiden hallintakyky on määritelty ja todennettu.
Perustason vaatimukset	1. Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi on organisoitu ja vastuutettu yhteistyön kohteeseen liittyen. 2. Havaituista kumppania koskevista tietoturvapoikkeamista tiedotetaan kumppanille välittömästi ja poikkeaman korjaustoimet aloitetaan sovitusti.
Korotetun tason lisävaatimukset	3. Tietoturvapoikkeaman käsittelystä yhteistyössä on kirjalliset ohjeet. 4. Poikkeamasta ja sen syystä valmistuu kirjallinen raportti. 5. Organisaatiokohtaisia jatkuvuusharjoituksia toteutetaan säännöllisesti
Korkean tason lisävaatimukset	6. Yhteistoimintaa erityistilanteessa harjoitellaan kumppanien kanssa. 7. Tietoa poikkeamien syistä käytetään sopimusten ja toiminnan parantamiseen.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 2: Alihankkijan kanssa on tehty palvelutasosopimus, jossa on määritelty, että poikkeamista tiedotetaan puhelimitse yhteyshenkilölle ja korjaustoimet aloitetaan sovitun ajan kuluessa. • Vaatimukseen 7: Alihankkijalla näkyi vahingossa testipalvelu julkiseen internetiin. Testijärjestelmän ja -aineiston luottamuksellisuutta ei alunperin ollut huomioitu sopimuksessa, joten se lisättiin sinne.
Apuvälineitä ja malleja	Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005) • Luku 2.2.5: Poikkeamatilanneharjoitukset ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin -yleisohje (VAHTI 2/2009)
Huomioita	Kunkin osapuolen vastuut yhteisessä poikkeamatilanteessa pitää sopia, sillä ne voivat poiketa organisaatioiden sisäisistä toimintamalleista. Kannattaa huomata, että poikkeama voi olla myös merkittävä palvelukatko.

1.5 Toiminnan prosesseille asetettavat vaatimukset

Osa-alueen nimi	1.5.1 Tietoaineistojen hallinta
Tavoitteet	Asiakirjallisen ja muun tietoaineiston turvallisuudesta huolehditaan sen koko elinkaaren aikana. Organisaatiossa käsitellään tietoaineistoja lakien ja hyvän hallintotavan mukaisesti.
Suomen erityisvaateet	1. Organisaatiolla on arkistonmuodostussuunnitelma (Arkistolaki 8§), josta käytetään usein myös nimitystä tiedonhallinta- tai tiedonohjaussuunnitelma. 2. Organisaatio pitää luetteloa organisaatioon käsiteltäviksi tulleista ja käsitellyistä asioista (Julkisuuslaki 18§).
Perustason vaatimukset	3. Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään. 4. Organisaation tuottamasta kirjallisesta asiakirjasta käy ilmi kuka sen on laatinut ja milloin sekä sen hyväksymisen tila. 5. Hävitettäväksi tarkoitetut asiakirjat tuhotaan niin, että luottamuksellisuus ja tietosuoja on varmistettu.
Korotetun tason lisävaatimukset	6. Organisaatiossa on tietoaineistojen käsittelyn kirjallinen ohje, jossa kerrotaan, miten asiakirjat hyväksytään, katselmoidaan ja mikä organisaation aineisto on salassa pidettävää tai muun vaitiolovelvollisuuden alaista.
Korkean tason lisävaatimukset	7. Organisaatiossa käytössä olevat tietoaineistojen hallinnan välineet tukevat aineistojen luokittelua ja arkistointia.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 3: Perehdyttämiskoulutuksessa otetaan esille perusasiat asiakirjojen käsittelystä. • Vaatimukseen 4: Organisaation dokumenttipohjassa on valmiiksi paikat laatijan sekä hyväksyjän nimille, päivämäärille, ja tehdyn muutoksen luonnehdinnalle.
Apuvälineitä ja malleja	Asianhallinnan tietoturvallisuutta koskeva ohje (VAHTI 5/2006) • Luku 9: Asianhallinnan tietoturvallisuuden tarkistuslista Arkistolaitoksen AMS-opas Arkistolaitoksen ohjeet ja mallit Lokiohje (VAHTI 3/2009)
Huomioita	Suomen erityisvaateet -osion vaatimuksia ei tarvitse toteuttaa yksityisen sektorin organisaatioissa.

1.6 Toiminnan arvioinnille ja todentamiselle asetettavat vaatimukset

Osa-alueen nimi	1.6.1 Toiminnan arviointi ja todentaminen
Tavoitteet	Tietoturvallisuuden hallinnan tilaa organisaatiossa seurataan jotta voidaan varmistua, että se palvelee ydintoimintaa.
Perustason vaatimukset	1. Organisaatiossa tehdään säännöllisesti tietoturvallisuuden auditointeja tai arviointeja. 2. Auditoinnit tai arvioinnit ovat suunniteltuja ja johdon hyväksymiä. 3. Auditoinnin tai arvioinnin tulokset raportoidaan toiminnon tai kohteen omistajalle. 4. Auditointien tai arviointien suosituksista pidetään koko organisaation tasolla kirjaa ja parannustoimenpiteiden toteutumista seurataan.
Korotetun tason lisävaatimukset	5. Tietoturva-auditointeja tai arviointeja tehdään joka vuosi. 6. Organisaatiossa on kirjallinen johdon hyväksymä auditointi- tai arviointiprosessi, jossa on mm. määritelty auditoijien tai arvioijien pätevyysvaatimukset. 7. Raportin pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa parannustoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle.
Korkean tason lisävaatimukset	8. Auditoinnit tai arvioinnit käyvät läpi organisaation ydintoiminnot 5 vuoden aikajaksolla. 9. Tietoturva-auditoinneissa tai -arvioinneissa käytetään myös ulkopuolisia resursseja.
Esimerkkejä hyvistä käytännöistä	• Vaatimukseen 1: Organisaatio voi tehdä oman vuosikellonsa mukaisesti. • Vaatimukseen 1: Organisaation päättämä toimija (esim. sisäinen tarkastus) tekee tietoturvallisuuteen liittyvän kokonaisarvioinnin esimerkiksi Vahti 8/2006 -ohjeen avulla. • Vaatimuksiin 1-2: Organisaation johto on hyväksynyt periaatteet, joiden mukaisesti yksiköt arvioivat joka toinen vuosi oman toimintansa tietoturvallisuutta ja raportoivat tuloksista. • Vaatimukseen 7: Organisaatiossa on luotu auditiontisuunnitelma, jonka mukaisesti vuonna 2010 auditoidaan organisaatiossa käyttövaltuuksien hallintaprosessit, vuonna 2011 kaikkien ulkoistus- ja palvelutasosopimusten tietoturvavaatimukset ja vuonna 2012 sähköisen asioinnin prosessit ja tietojärjestelmät.
Apuvälineitä ja malleja	Katso kaikki VAHTI-ohjeet www.vm.fi/vahti ja erityisesti 1/2009 Tietoturvallisuuden arviointi valtionhallinnossa (VAHTI 8/2006) • Hallinnollisen turvallisuuden RTF-arviointipohja • Henkilöstöturvallisuuden RTF-arviointipohja • Fyysisen turvallisuuden RTF-arviointipohja • Tietoliikenneturvallisuuden RTF-arviointipohja • Ohjelmistoturvallisuuden RTF-arviointipohja • Laitteistoturvallisuuden RTF-arviointipohja • Tietoaineistoturvallisuuden RTF-arviointipohja • Käyttöturvallisuuden RTF-arviointipohja • Jatkuvuussuunnittelun RTF-arviointipohja • Valmiussuunnittelun RTF-arviointipohja • Ulkoistamisen RTF-arviointipohja CAF-arviointimalli www.vm.fi/caf/ Valtiokonttorin VIPin auditointipalvelun asiantuntijat ovat käytettävissä arviointiin www.valtiokonttori.fi/vip/
Huomioita	Auditoinnissa tai arvioinnissa tietoturvallisuutta ja sen hallintaa tulee katsoa ydintoimintojen vaatimuksia palvelevana kokonaisuutena. Näitä voidaan toteuttaa mm suorittamalla erilaisia teknisiä tietoturvatarkastuksia ja itsearviointeja. Viranomainen voi varmistaa järjestelmiensä tietoturvallisuustason käyttämällä arviointipalveluja, joissa viranomaisen tietoturvallisuustoimien taso arvioidaan suhteessa tietoturvallisuusasetukseen ja näihin ohjeisiin taikka, jos kysymys on esim. EU-asiakirjojen käsittelystä, suhteessa EU:n turvallisuussääntöihin. Tietoturvallisuuden kannalta olennaista on se, että arviointien ja auditointien tulokset käsitellään ja niiden pohjalta parannetaan toimintaa.

2 Tietojärjestelmien hallinnan vaatimukset

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.

2.2 Omaisuuden hallinta

Osa-alueen nimi	2.2 Omaisuuden hallinta
Tavoitteet	Organisaation vastuulla olevat laitteet, ohjelmistot ja rekisterit sekä niistä koostuvat tietojärjestelmät on tunnistettu, jotta niiden turvallisuudesta voidaan huolehtia.
Suomen erityisvaateet	1. Organisaation omistamista henkilörekistereistä on Henkilötietolain 10§ mukainen rekisteriseloste ja se on asetettu rekisteröityjen nähtäville. 2. Kustakin tietojärjestelmästä on Julkisuuslain 18§ mukainen tietojärjestelmäkuvaus.
Perustason vaatimukset	3. Organisaatiossa on luettelot organisaation omistamista ja käyttämistä fyysisistä tai virtuaalisista laitteista, tietojärjestelmistä, palveluista sekä ohjelmistoista ja lisensseistä. 4. Laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu. 5. Laite-, tietojärjestelmä-, palvelu- ja ohjelmistoluettelojen sekä lain mukaisten selosteiden ja kuvausten päivitys on organisoitu ja vastuutettu.
Korotetun tason lisävaatimukset	6. Omistaja on dokumentoinut laitteiden, tietojärjestelmien ja rekistereiden tietosisällön. 7. Omistaja on luokitellut omaisuuden tarvittavan tietoturvallisuustason mukaisesti. 8. Omistajat katselmoivat laite-, rekisteri-, palvelu- ja ohjelmistoluetteloiden sekä lain mukaisten selosteiden ja kuvausten sisällön säännöllisesti.
Korkean tason lisävaatimukset	-
Käytännön esimerkkejä	• Vaatimukseen 1: Organisaation asiointipalvelun käyttäjärekisterin seloste on nähtävissä julkisessa Internetissä. • Vaatimukseen 3: Organisaatio on hankkinut käyttöönsä virtuaalipalvelimia palveluntarjoajalta. Virtuaalipalvelimien kirjanpito saadaan tällöin käyttöpalvelutoimittajalta. • Vaatimukseen 4: Organisaation asianhallintajärjestelmän omistaa hallintopalveluyksikkö ja tietoverkkoinfrastruktuurin tietohallinto. Yksiköt nimeävät sisältään henkilöt, joille omistajarooli kuuluu. • Vaatimukseen 5: Kun uusi työasema otetaan käyttöön, työasematuen vastuulla on kirjata laite tietoineen työasemien laiteluettelona toimivaan Excel-taulukkoon. • Vaatimukseen 7: Organisaatiossa on kaksi tietojärjestelmää: matkahallintajärjestelmä korotetulla tietoturvallisuustasolla ja asiointijärjestelmä korkealla tietoturvallisuustasolla. Kummankin järjestelmän taustalla olevat tietokannat toimivat resurssien tarkoituksenmukaisen käytön vuoksi samalla fyysisellä tietokantapalvelimella. Tietokantapalvelimen tietoturvallisuustason tulee tällöin olla korkealla tasolla. • Vaatimukseen 7: Tietojärjestelmät on luokiteltu sekä tietoturvallisuustason mukaisesti että sen mukaan kuinka välttämättömiä ne ovat organisaation toiminnalle.
Apuvälineitä ja malleja	Henkilörekisteriselosteen RTF-lomakepohja, www.tietosuoja.fi Tietojärjestelmäselosteen RTF-lomakepohja, www.tietosuoja.fi
Huomioita	Olennaista on tunnistaa suojattavat tekniset kohteet. Liitteen 1 kohdissa Tavoitteiden määrittely ja Toimintaympäristön vaikutus käsiteltiin samaa asiaa organisaation päätoimintojen näkökulmasta. Tässä osiossa mennään syvemmälle ICT-tekniikkaan, sillä pelkkä päätoimintojen näkökulma ei ole kokonaistietoturvallisuuden kannalta riittävän tarkka. Suojattavien kohteiden tunnistamisen lisäksi on kohteille oltava omistaja, jolla on oikeus tehdä kohdetta koskevia käytännön päätöksiä (esim. riskitaso, käyttöönotto, poistaminen ja asennusmuutokset). Omistaja voi olla organisaatioyksikkö; yksikön sisällä tulisi määritellä myös omistajaroolien haltijat.

2.3 Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto

Osa-alueen nimi	2.3 Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto
Tavoitteet	Tietojenkäsittely-ympäristöt, lähinnä tietojärjestelmät ja työasemat otetaan käyttöön ja poistetaan käytöstä turvallisesti elinkaarenhallintaprosessin mukaisesti.
Perustason vaatimukset	1. Tietojärjestelmän ja työasemien käyttöönottoasennuksessa ja käytöstä poistamisessa otetaan huomioon järjestelmän tietosisällön tietoturvavaatimukset. 2. Tietojärjestelmien ja työasemien käyttöönottoon ja käytöstä poistamiseen liittyvät toimenpiteet on vastuutettu ja organisoitu.
Korotetun tason lisävaatimukset	3. Tietojärjestelmien ja työasemien ensiasennuksesta ja käytöstä poistosta on kirjallinen ohjeisto, jossa kerrotaan mm. eri turvatasoilla käytettävät tietoturva-asetukset sekä laitteiden käsittelyn ja massamuistien tyhjennyksen menettelyt silloin kun ne siirtyvät ympäristöstä toiseen tai kun ne poistuvat organisaation hallinnasta. 4. Ohjeiden päivitys on vastuutettu ja organisoitu.
Korkean tason lisävaatimukset	5. Korkean tietoturvallisuustason tietojärjestelmät ja työasemat kovennetaan. 6. Tietojärjestelmät ja työasemat huolletaan niin, että massamuisteilla olevat tiedot eivät joudu ulkopuolisten haltuun.
Käytännön esimerkkejä	• Vaatimuksiin 1 ja 3: Organisaatiossa työasemapalvelut on hankittu ulkopuoliselta palveluntarjoajalta, joka vastaa ensiasennuksista ja käytöstä poistamisesta sopimuksen tietoturvaliitteessä olevien teknisten ohjeiden mukaisesti. • Vaatimuksiin 2-3: Käyttöpalvelut ulkoistaneessa organisaatiossa on alihankkijan kanssa yhdessä tehty tietojärjestelmän asennusohje, jossa kerrotaan miten eri tietojärjestelmäalustat oletusarvoisesti asennetaan ja mitä tietoturvapiirteitä käytetään eri tietoturvallisuustason järjestelmissä mm. lokituksen, salasanojen ja käytössä olevien palveluiden osalta. • Vaatimukseen 5: Organisaatiossa on sovittu, että Solaris-käyttöjärjestelmän tietoturva-asetukset kovennetaan käyttämällä Solaris security toolkit -työkalua ja Windows Server 2003 -järjestelmät käyttämällä CIS:in ohjeiden perusteella tehtyä Group Policyä.
Apuvälineitä ja malleja	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004) • Luku 12: Käyttöturvallisuus Haittaohjelmilta suojautumisen yleisohje (VAHTI 3/2004) • Luku 5.1: Työaseman turvalliset asetukset NIST:in teknisiä järjestelmien ylläpito- ja konfigurointiohjeita NIST:in teknisiä järjestelmien tietoturvallisuuden tarkistuslistoja Center for Internet Security: eri järjestelmien koventamisohjeita • Ohjeet ovat ilmaisia mutta vaativat rekisteröitymisen. Darik's Boot and Nuke, ilmainen levyn tyhjennysohjelma.
Huomioita	Järjestelmien teknisen tietoturvallisuuden yksi kulmakivi on huolellinen tietoturvallisuuden huomioon ottava perusasennus. Ylläpitoa helpottaa, että järjestelmät ovat mahdollisimman samanlaisia. Korkean tietoturvallisuustason järjestelmissä on syytä käyttää koventamista, jolla kiristetään tietoturvallisuuteen vaikuttavia oletusasetuksia. Koventamisohjeita löytyy erilaisiin käyttöjärjestelmiin, tietokantoihin sekä reitittimiin USA:n NIST:iltä ja CIS:ltä. Tietovuotojen ehkäisemiseksi on myös syytä huolehtia, että käytöstä poistettujen laitteiden levyt päällekirjoitetaan tai tuhotaan luotettavasti ennen niiden poistumista organisaation hallinnasta.

2.4 Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta

Osa-alueen nimi	2.4 Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta
Tavoitteet	Tietojenkäsittely-ympäristöt päivitetään hallitusti, jotta estetään haavoittuvuuksien hyväksikäyttö ja tietoturvaongelmien synty.
Perustason vaatimukset	1. Laitteiden ja tietojärjestelmien päivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on vastuutettu ja organisoitu erityisesti tietoturvapäivitysten osalta. 2. Laitteiden ja tietojärjestelmien muutostarpeen seuranta, muutospäätösten teko ja muutosten toteutus on vastuutettu ja organisoitu. 3. Organisaatiolla on periaatteet, jotka kertovat, millaiset päivitykset tai muutokset asennetaan välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa.
Korotetun tason lisävaatimukset	4. Muut kuin päivitys- ja muutoshallintaperiaatteiden perusteella kiireellisinä toteutettavat päivitykset tai muutokset tehdään vain etukäteen sovittuna aikana (ns. huoltoikkuna). 5. Tietojärjestelmään saadaan asentaa tai liittää vain järjestelmän omistajan hyväksymiä ohjelmia ja laitteita. 6. Organisaation päivitys- ja muutosperiaatteet ovat kirjalliset.
Korkean tason lisävaatimukset	7. Päivitysten ajantasaisuutta ja onnistumista mitataan ja seurataan. 8. Päivitykset ja muutokset testataan ennen kuin ne otetaan tuotantokäyttöön. 9. Organisaatiossa osallistutaan tietoturvatilanteen seuranta- tai yhteistyöryhmiin.
Käytännön esimerkkejä	• Vaatimuksiin 1-3: Organisaatiossa on otettu käyttöön ITIL Change Management -muutoksenhallintakäytännöt. • Vaatimukseen 1: Työasematuen vastuulle on annettu Windows XP ja Office -ympäristöjen tietoturvatilanteen seuraaminen. Organisaation Linux- ja Apache -ympäristöjen päivitysseuranta on vastuutettu palvelinylläpitoryhmälle. Päivityspäätöksen palvelinten osalta tekee käyttöpäällikkö, työasemat päivittyvät automaattisesti. • Vaatimukseen 2: Organisaatiossa on yhteinen työasemien perusasennus. Lisäksi on sovittu, että esimiehen luvalla työasemiin voidaan asentaa tiettyjä lisäsovelluksia. • Vaatimukseen 4: ICT-palveluorganisaatiolla on huoltoikkuna joka viikon torstai-iltana klo 19-21, jolloin tarvittavat päivitykset voidaan asentaa ja muutokset tehdä tuotannon häiriytymättä liikaa. • Vaatimukseen 7: Työasematuki käyttää ohjelmistoa, jolla se voi seurata, monellako prosentilla organisaation työasemista tietty päivitys on. • Vaatimukseen 9: Organisaatiossa seurataan CERT-FI -postituslistaa ja osallistutaan hallinnon tietoturvahenkilöstön yhteiskokouksiin.
Apuvälineitä ja malleja	Keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004) • Luku 12.4: Muutosten hallinta Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005) • Luku 2.1.8. Tietojärjestelmien turvallinen ylläpito Haittaohjelmilta suojautumisen yleisohje (VAHTI 3/2004) • Luku 5.2: Ohjelmistohaavoittuvuudet ja korjauspäivitykset
Huomioita	Edellisessä osiossa teknisen tietoturvallisuuden perusta laskettiin tietoturvallisuuden huomioon ottavan vakioidun asennuksen varaan. Tietoturvallisuustaso murenee kuitenkin pikaisesti, jos muutoksia käyttöjärjestelmään tai ohjelmistoihin tehdään hallitsemattomasti tai tietoturvapäivityksiä ei asenneta ollenkaan. Organisaatioissa on käytössä erilaisia tietojärjestelmiä. Jotkin järjestelmät ovat esim. sijaintinsa takia alttiimpia hyökkäyksille kuin toiset. Joihinkin päivitysten teko on hyvin yksinkertaista, joihinkin haastavaa esimerkiksi käytettävyysvaatimusten tai ohjelmistotoimittajan tuen puutteen vuoksi. Olennaista on se, että päivitysten suhteen haastavat järjestelmät on tunnistettu ja mietitty millä tavoin päivitykset, erityisesti kriittiset tietoturvakorjaukset, tehdään. Jos päivittäminen ei ole mahdollista, omistajan tulee miettiä mitä muita toimenpiteitä voidaan tehdä riskin pienentämiseksi. Tietojärjestelmien ja sovellusten kehittämistä käsitellään jäljempänä osiossa "Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta".

2.5 Turva-alueiden muodostus ja niiden välinen suodatus

Osa-alueen nimi	2.5 Turva-alueiden muodostus ja niiden välinen suodatus
Tavoitteet	Tieto kulkee tietoverkosta toiseen vain valtuutetusti.
Perustason vaatimukset	1. Organisaatiossa on tunnistettu ja eriytetty tietoverkon eri suojaustasoa vaativat osat ja eri suojaustason verkkojen välistä liikennettä rajoitetaan ja suodatetaan. 2. Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden tietoliikennelaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 3. Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu. 4. Julkisesta verkosta organisaatioon sisäänpäin tulevaa liikennettä rajoitetaan ja suodatetaan ”kaikki liikenne on kielletty ellei erikseen sallittu” -periaatteella. Myös organisaatiosta julkiseen verkkoon lähtevää liikennettä suodatetaan. 5. Organisaatiossa on etäkäyttöperiaatteet.
Korotetun tason lisävaatimukset	6. Organisaatiossa on kirjallinen palomuuri- ja liikenteensuodatuspolitiikka sekä kirjallinen sääntöjen päivitysprosessi. 7. Palomuurien tai muiden suodatuslaitteiden säännöstöjen ajantasaisuutta katselmoidaan säännöllisesti. 8. Tietoverkkoihin saadaan liittää vain verkon omistajan hyväksymiä laitteita. 9. Etäkäyttöperiaatteet ovat kirjalliset. Periaatteissa kerrotaan minkälaisilla laitteilla ja mistä verkoista yhteyttä voidaan ottaa sekä mitä järjestelmiä käyttää ja ylläpitää.
Korkean tason lisävaatimukset	10. Tietoverkkoja valvotaan tietoturvapoikkeamien ja -loukkausten varalta ja havaittuihin poikkeamiin reagoidaan.
Käytännön esimerkkejä	• Vaatimukseen 1: Organisaatiolla on eriytetty kolme loogisesti erillistä tietoverkkosegmenttiä: julkisia palveluita sisältävä puoliluotettu verkko (ns. DMZ), työasemat sisältävä työasemaverkko sekä tietovarastoja ja palvelimia sisältävä palvelinverkko, jotka on eristetty palomuurilla. • Vaatimukseen 2: Organisaatiossa on sovittu, että ainoastaan tietoturvapäällikkö saa lähettää tietoliikenteen palveluntarjoajalle muutospyyntöjä julkisen verkon palomuuriin. • Vaatimukseen 3: Jokaisesta ulkoisen palomuurin avaussäännöstä on kirjattu palomuurin hallintakäyttöliittymän sääntökohtaiseen kommenttikenttään avauspyynnön tekijä, pyynnön syy sekä voimassaoloaika • Vaatimukseen 8: Palvelinverkon omistajalta tulee pyytää aina lupa uuden palvelimen kytkemiseen. WLAN-vierailijaverkon omistaja on linjannut, että siihen saa liittää organisaatiossa vierailevien tietokoneita. • Vaatimukseen 10: Korkean suojaustason tietoverkossa käytetään loukkausten havaitsemiseen ja torjuntaan IDS/IPS-järjestelmää.
Apuvälineitä ja malleja	Valtion tietohallinnon Internet-tietoturvallisuusohje (VAHTI 1/2003) • Luku 3.2 Yhteys Internetiin Turvallinen etäkäyttö turvattomista verkoista (VAHTI 2/2003) Haittaohjelmilta suojautumisen yleisohje (VAHTI 3/2004) • Luku 5.4: Organisaation verkon suojaaminen • Luku 5.5: Työskentely organisaation ulkopuolella
Huomioita	Valtion yhteisen tietoliikenneverkon käyttöönoton jälkeen suurin osa ulkoisia tietoliikenneyhteyksiä koskevista vaatimuksista täyttyy automaattisesti verkon käyttäjäorganisaatioissa. Tietoverkoista tulevien uhkien torjunnassa verkkojen toiminnallinen eriyttäminen ja liikenteen suodatus on olennaista. Teknisesti tämä on varsin yksinkertaista, mutta palomuurien ja niiden suodatussääntöjen hallinta on varsin yleinen ongelma. Erityisesti ulkoistustilanteessa on hyvin selkeästi sovittava kuka saa tehdä muutoksia, minkä tietojen perusteella ja kenellä on vastuu mistäkin ylläpitoprosessin osasta. Esimerkiksi palveluntarjoaja ei voi tehdä pyydetyn muutoksen asiatarkastusta, ainoastaan teknisen tarkastuksen ja toteutuksen.

2.6 Pääsynvalvonta

Osa-alueen nimi	2.6 Pääsynvalvonta
Tavoitteet	Tietoon pääsevät käsiksi vain valtuutetut käyttäjät.
Perustason vaatimukset	1. Tietojärjestelmän omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan. 2. Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti. 3. Huonolaatuisten salasanojen käyttöä estetään.
Korotetun tason lisävaatimukset	4. Organisaatiossa on kirjallinen pääsynvalvontapolitiikka, jossa kerrotaan mm. eri turvatasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet. 5. Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan. 6. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.
Korkean tason lisävaatimukset	7. Varmenteiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista varmenteista ajantasainen lista. 8. Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti. 9. Tunnistuksen epäonnistumista sekä muita valtuuksien puutteeseen kariutuvia toimenpideyrityksiä tilastoidaan.
Käytännön esimerkkejä	• Vaatimukseen 1: Organisaatiossa on riskianalyysin avulla todettu, että WLAN-vierailijaverkon käyttöön ei tarvita tunnistusta, sillä siitä ei teknisesti pääse organisaation sisäverkon suojattaviin tietoihin, työasemien käyttöön riittää käyttäjätunnus/salasana -pari, mutta organisaation henkilöstö- ja palkanmaksujärjestelmään tarvitaan tunnistus virkakortilla. • Vaatimukseen 1: Organisaatiossa on järjestelmien omistajien hyväksymä järjestelmien tärkeysluokitus, jonka perusteella vaadittava tunnistuksen vahvuus määräytyy. • Vaatimukseen 1: Organisaation verkkopalveluille on määritelty eri tunnistustavat VAHTI 12/2006-ohjeen mukaisesti. Tietohallinto esittelee ehdotuksen järjestelmien omistajayksiköille, joka hyväksyy ehdotuksen jos se on linjassa järjestelmien sisältämien tietojen vaatimusten kanssa. • Vaatimukseen 3: Organisaatiossa on kirjallisesti ohjeistettu hyvä salasanakäytäntö salasanan vähimmäispituuksineen. Sen lisäksi niissä tietojärjestelmissä, joissa se on mahdollista, on otettu salasanan laatutarkistus käyttöön. • Vaatimukseen 8: Terveystietojärjestelmä lokittaa myös sen, kuka on käynyt katsomassa kenenkin sairauskertomuksia, jotta voidaan tarvittaessa selvittää, onko henkilöllä ollut tarve nähdä tiedot.
Apuvälineitä ja malleja	Käyttövaltuushallinnan periaatteet ja hyvät käytännöt (VAHTI 9/2006). Tunnistaminen julkishallinnon verkkopalveluissa (VAHTI 12/2006) • Luvut 4.2-4.3: Käyttäjien tunnistamisen luotettavuus ja Palvelutyyppien edellyttämä käyttäjän tunnistamisen luotettavuus. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008) • Luku 4.12 Pääsyn hallinta ja tunnistaminen
Huomioita	Pääsynvalvonta on käytännön tietoturvatoimenpiteistä tärkeimpiä. Eduksi on, jos organisaatiossa olisi yhteiset periaatteet tunnistukseen ja pääsynvalvontatietojen lokitukseen, mutta järjestelmäkohtaiset periaatteet ovat myös hyväksyttäviä silloin kun yhteisesti sovittua tapaa ei esimerkiksi teknisistä syistä voida toteuttaa. On todennäköistä, että järjestelmän omistajana toimivalla yksiköllä ei ole tarvittava asiantuntemusta konkreettisten teknisten menetelmäpäätösten tekoon. Tällöin tietotekniset asiantuntijat esittelevät vaihtoehdot ja niiden riskitasot ja omistajataho hyväksyy vaihtoehdoista parhaiten sopivan. Käyttäjän ensirekisteröitymistä organisaation järjestelmien käyttäjäksi ja käyttövaltuuksien myöntöä käsitellään osiossa G.

2.7 Käyttäjien ja käyttövaltuuksien hallinta

Osa-alueen nimi	2.7 Käyttäjien ja käyttövaltuuksien hallinta
Tavoitteet	Käyttäjätunnukset ja käyttövaltuudet ovat yhdistettävissä niitä käyttävin henkilöihin.
Perustason vaatimukset	1. Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet. Tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu periaatteiden mukaisesti. 2. Käyttövaltuudet ovat henkilö- tai roolikohtaisia. 3. Käyttövaltuudet perustuvat palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä. 4. Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää. 5. Uuden henkilön tullessa organisaatioon ensimmäinen tunnistus tehdään valokuvallisesta henkilöllisyystodistuksesta tai sähköiseen palveluun rekisteröitymisen osalta käyttäen samantasoista todennusmenetelmää.
Korotetun tason lisävaatimukset	6. Organisaatiossa on kirjallinen käyttövaltuuspolitiikka ja hallintaprosessi. 7. Jokaisella käyttövaltuudella on omistaja. 8. Järjestelmien käyttövaltuudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet suljetaan tai poistetaan. 9. Myöntöprosessista jää jälki, millä perusteella käyttäjälle on myönnetty käyttövaltuus. 10. Kielletyt työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään.
Korkean tason lisävaatimukset	11. Ylläpito- ja pääkäyttäjäoikeuksien määrää seurataan ja tilastoidaan. 12. Käyttövaltuuksien poistoon kuluvaa aikaa seurataan ja tilastoidaan. 13. Organisaatiossa on dokumentoitu menettely käyttäjätunnuksen tai käyttövaltuuksien välittömään poistoon tai passivointiin.
Käytännön esimerkkejä	• Vaatimukseen 1: Organisaatiossa on sovittu, että kaikki virka- tai työsopimussuuhteessa olevat saavat automaattisesti käyttöönsä työasematunnuksen, tunnuksia sovelluksiin tai palvelimiin annetaan vain esimiehen katsoessa sen työtehtävien osalta tarpeelliseksi. • Vaatimukseen 2: Virtu-luottamusverkostoon kytketyt työasemakäyttäjätunnukset ovat henkilökohtaisia. • Vaatimukseen 3: Suuressa organisaatiossa on käytössä automatisoitu identiteetinhallintajärjestelmä, jonka avulla henkilön käyttäjätunnukset poistetaan automaattisesti kun henkilön työ- tai virkasuhde päättyy. • Vaatimukseen 5: Potentiaalisen työntekijän henkilöllisyys tarkastetaan jo haastatteluvaiheessa valokuvallisesta henkilöllisyystodistuksesta. Sähköisessä asioinnissa käyttäjäksi voi rekisteröityä pankkitunnuksin. • Vaatimukseen 7: Organisaatiossa on sovittu, että järjestelmän omistaja omistaa myös siihen järjestelmään tehdyt valtuudet olivatpa ne sitten henkilö- tai roolikohtaisia tai teknisten järjestelmien välisiä tunnuksia.
Apuvälineitä ja malleja	Käyttövaltuushallinnan periaatteet ja hyvät käytännöt (VAHTI 9/2006). • Luku 2.2: Käyttövaltuusrekisterin suunnitteluvaatimus. • Luku 3: Hyvän käyttövaltuushallinnon edellytysten luominen. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008) • Luku 4.5: Valtuuttaminen
Huomioita	Organisaatiossa olisi hyvä olla kaikki järjestelmät kattavat käyttövaltuuksien hallintapolitiikka ja -prosessi, mutta jos se ei ole mahdollista, tulisi periaatteet ja prosessit tehdä tietoturvallisuustasokohtaisiksi. Järjestelmäkohtaisia toteutuksia tulisi välttää, koska niiden ylläpito ja jalkauttaminen vie yhteisiä periaatteita enemmän resursseja. Suurin osa tässä mainituista toimenpiteistä ei ole IT-osaston toiminta-alueella, vaan niiden tulisi olla osa henkilöstöhallinnon prosesseja.

2.8 Haittaohjelmasuojaus

Osa-alueen nimi	2.8 Haittaohjelmasuojaus
Tavoitteet	Organisaation tietovarannot ovat suojassa haittaohjelmien (virukset, vakoiluohjelmat, takaportit jne.) aiheuttamilta vahingoilta.
Perustason vaatimukset	1. Organisaatiossa suodatetaan haittaohjelmia sekä työasematasolla että kaikissa sähköpostin ja www-liikenteen sisääntulo- ja ulosmenopisteissä. 2. Haittaohjelmakuvaukset päivittyvät säännöllisesti ja automaattisesti.
Korotetun tason lisävaatimukset	3. Käyttäjiä on ohjeistettu, miten haittaohjelmia levittäviä sähköposteja voidaan yrittää tunnistaa ja mitä tehdä haittaohjelmaepäilytilanteessa. 4. Haittaohjelmistokuvausten ajantasaisuutta valvotaan.
Korkean tason lisävaatimukset	5. Työasema ei saa kytkeytyä korkean tietoturvallisuustason verkkoihin, ellei ole varmistettu että se on puhdas haittaohjelmista. 6. Haittaohjelmasuodatuksen kattavuutta mitataan ja seurataan.
Käytännön esimerkkejä	• Vaatimus 1: Organisaatiossa on riskianalyysin avulla todettu, että työasematasolla tarvitaan haittaohjelmasuojausta ainoastaan Windows-pohjaisissa työasemissa ja niissä älypuhelimissa, joissa on käytössä organisaation sähköposti- ja kalenteripalvelut. Lisäksi sähköpostipalvelimeen ja www-välityspalvelimeen asennetaan haittaohjelmasuodatus.
Apuvälineitä ja malleja	Haittaohjelmilta suojautumisen yleisohje (VAHTI 3/2004) • Luku 5: Kuinka välttää tartunta • Liite 3: Käyttäjän pikaopas ISO/IEC27002-standardi • 10.4, 10.6 ja
Huomioita	Haittaohjelmia leviää usean eri kanavan kautta, sähköposti ja www-sivut ovat tyypillisimpiä, mutta eivät suinkaan ainoita. Haittaohjelmasuodatuksen lisääminen www-yhteyspisteisiin voi vaatia rahallisia lisäpanostuksia, mutta todennäköisesti vähentää haittaohjelmien siivouksen aiheuttamaa työmäärää. Räätälöityjen haittaohjelmahyökkäysten tunnistus ja torjunta on teknisesti vaikeaa. Tämän vuoksi käyttäjien valistaminen ongelmasta on hyvin tärkeää.

2.9 Fyysisen ympäristön suojaus

Osa-alueen nimi	2.9 Fyysisen ympäristön suojaus
Tavoitteet	Tietoturvariskien realisoituminen estetään käyttämällä myös sopivia fyysisen turvallisuuden menetelmiä.
Perustason vaatimukset	1. Organisaatiossa on tunnistettu omien tilojen tarvitsema suojausluokka ja eriytetty eri suojausluokkaa vaativat osat rajoittamalla kulkua tilojen välillä. 2. Organisaatiossa on sovittu henkilö- tai roolitasolla, kenellä on pääsy IT-laitetiloihin ja kulunvalvonta on organisoitu tämän mukaisesti.
Korotetun tason lisävaatimukset	3. Tilojen eriytys eri suojausluokkiin on dokumentoitu. 4. Tietoliikennelaitteiden, -yhteyksien ja kytkentäpisteiden sijainti on otettu huomioon suojausluokittelussa.
Korkean tason lisävaatimukset	5. Tiloja ja niissä kulkua valvotaan automaattisesti ja valvontamenettely on dokumentoitu. 6. Ulkopuolisten toimintaa IT-laitetiloissa valvotaan.
Käytännön esimerkkejä	• Vaatimuksiin 1 ja 4: Organisaation käytössä olevasta saunaosastosta poistettiin käytöstä sisäverkon tietoliikennepistoke, sillä saunaosastoa vuokrattiin myös täysin ulkopuolisten käyttöön.
Apuvälineitä ja malleja	Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa (VM 1/01/1999) Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007) • Luku 12.2: Toimitilojen luokitus. Teknisten laitetilojen turvallisuussuositus (VAHTI 1/2002) • Luku 3: IT-laitetilojen tietoturvatoimenpiteet osa-alueittain. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008) • Liite 5: Pääsyn hallinnan toteuttaminen EU määräyksen mukaisesti Suojarakentamisen vaatimukset • S1-S3, Sisäisen turvallisuuden ohjelma STOII
Huomioita	Tämä vastaa tietoverkon eriyttämistä fyysisen turvallisuuden puolella.

2.10 Varmuuskopiointi

Osa-alueen nimi	2.10 Varmuuskopiointi
Tavoitteet	Tiedon hallitsematon katoaminen organisaatiosta estetään ja vähennetään erilaisten häiriötilanteiden vaikutusta organisaation toimintaan.
Perustason vaatimukset	1. Organisaatiossa on vastuutettu ja organisoitu varmuuskopioiden ottaminen. 2. Organisaatiossa on tunnistettu varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti. Myös varmuuskopioiden palauttaminen on suunniteltu.
Korotetun tason lisävaatimukset	3. Organisaatiossa on kirjallinen varmuuskopiointipolitiikka ja -prosessi, jotka on muodostettu ottaen huomioon toiminnan vaatimukset ja joissa ohjeistetaan varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana. 4. Organisaatiossa otetaan tärkeimmistä järjestelmistä suojakopioita, joita säilytetään eri palotilassa kun varsinaisia varmuuskopioita.
Korkean tason lisävaatimukset	5. Eri järjestelmien varmuuskopioiden palautusta testataan säännöllisesti. 6. Varmuuskopioilta palautettavien tietojen määrää ja palautuksen syitä tilastoidaan.
Käytännön esimerkkejä	• Vaatimukseen 2: Organisaatiolla, jolle tietoliikenneinfrastruktuuri on kriittinen suojattava kohde, varmuuskopioidaan myös reitittimien ja muiden verkon aktiivilaitteiden konfiguraatiot. • Vaatimukseen 3: Korkean tason tietojärjestelmästä otetaan joka viikko täysvarmistus ja joka yö varmistetaan muuttuneet tiedot, sillä järjestelmän vaatimuksena on kyky palata virheen jälkeen edellisen päivän tilanteeseen. Järjestelmän salaamaton suojakopio voidaan siirtää toiseen rakennukseen vain oman työntekijän saattamana. • Vaatimukseen 5: Kerran puolessa vuodessa testataan jonkin varmistustaltion palautusta testilaitteeseen.
Apuvälineitä ja malleja	Työeläkelaitoksen (TELA) vakuutustoimialan suositus • suojakopioiden ottaminen
Huomioita	Varmuuskopiointipolitiikat voivat olla järjestelmäkohtaisia. Suojakopiolla tarkoitetaan järjestelmän täysvarmistusta, joka on tarkoitettu pitkäaikaissäilytykseen. Varmuuskopioinnin suunnittelussa on tärkeää, mitä varmuuskopioidaan ja kuinka usein (tietokanta, ohjelmisto asetuksineen, käyttöjärjestelmä). Lisäksi on huomattava jatkuvuus- ja toipumissuunnitelmien aikarajat. Organisaation toiminnan jatkuvuuden varmistamista käsitellään liitteen 1 ”Erityistilanteiden hallinta” -osiossa. ICT-järjestelmien toipumissuunnittelua käsitellään jäljempänä osassa ”Tietojärjestelmien toipuminen häiriöistä”.

2.11 Tietoturvapoikkeamien valvonta

Osa-alueen nimi	2.11 Tietoturvapoikkeamien valvonta
Tavoitteet	Tietoturvapoikkeamat voidaan havaita ja selvittää.
Suomen erityisvaateet	1. Sähköisten viestien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös lokitietojen käsittelyssä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§).
Perustason vaatimukset	2. Laitteet, ohjelmistot sekä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan.
Korotetun tason lisävaatimukset	3. Organisaatiossa on kirjallinen lokienkeräys-, hälytys- ja seurantapolitiikka, joka on muodostettu ottaen huomioon toiminnan vaatimukset.
Korkean tason lisävaatimukset	4. Lokien seurannan perusteella muodostetaan tilannekuvaa ja havaitaan tietoturvapoikkeamia sekä kehitetään toimintaa.
Käytännön esimerkkejä	• Vaatimuksiin 2 ja 3: Organisaatiossa kaikki laitteet ja tietojärjestelmät kirjoittavat lokinsa keskitettyyn lokipalvelimeen, josta tarvittaessa ylläpito selvittää häiriöiden ja tietoturvapoikkeamien syitä.
Apuvälineitä ja malleja	Asianhallinnan tietoturvallisuutta koskeva ohje (VAHTI 5/2006) • Luku 5: Loki- ja muutoshistoriatiedot. Lokiohje (VAHTI 3/2009) ISO/IEC 27002 • 10.10 Monitoring
Huomioita	Aikaisemmin Omaisuuden hallinta -osiossa on selvitetty, mitä laitteita, ohjelmistoja ja järjestelmiä organisaatiossa on. Konkreettinen lokiohjeistus voi olla järjestelmä- tai alustakohtainen, mutta organisaatiolla tulisi olla yleisperiaatteet siitä mitä lokitetaan, minne ja kuinka pitkäksi aikaa sekä minkälaisista signaaleista ylläpitäjille tulee lähteä välitön hälytys. Lokien seurannan automatisointi säästää henkilökustannuksia. Tietoturvapoikkeamien käsittelyyn liittyviä vaatimuksia on kuvattu myös liitteessä 1 osioissa ”Johtaminen erityistilanteissa” sekä ”Erityistilanteissa toimiminen”.

2.12 Tietojärjestelmien toipuminen häiriöistä

Osa-alueen nimi	2.12 Tietojärjestelmien toipuminen häiriöistä
Tavoitteet	ICT-järjestelmiä kohtaaviin häiriöihin varaudutaan, jotta järjestelmät toipuvat häiriöistä riittävän nopeasti.
Suomen erityisvaateet	1. ICT-järjestelmien omistajat tietävät ICT-varautumiseen liittyvät vastuunsa ja toiminta on organisoitu ja vastuutettu sen mukaisesti.
Perustason vaatimukset	2. ICT-järjestelmien häiriöiden selvitys ja niistä toipuminen on organisoitu ja vastuutettu. 3. Organisaatiossa on yleinen toipumisstrategia ja suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille.
Korotetun tason lisävaatimukset	4. Organisaatiolla on tärkeimmistä järjestelmistä kirjalliset toipumissuunnitelmat.
Korkean tason lisävaatimukset	5. Järjestelmien häiriöistä ja niiden syistä pidetään kirjaa. Tietoa käytetään hyväksi riskianalyyseissä ja palvelutasosopimusten teossa.
Käytännön esimerkkejä	• Vaatimukseen 2: Organisaatiossa tietohallinnon käyttöpäällikkö vastaa ICT-palveluiden sujuvasta toiminnasta. Käyttöpäällikkö on nimennyt kullekin ICT-palvelulle teknisen vastaavan, jonka tehtävänä on tarvittaessa ryhtyä toipumissuunnitelman mukaisiin toimenpiteisiin. • Vaatimukseen 3: Organisaatiossa on valittu yleiseksi toipumisstrategiaksi palveluiden ulkoistus ja riittävät palvelutaso-sopimukset. Toipumissuunnitelmien valmistelusta vastaa tällöin palveluntarjoaja. • Vaatimukseen 4: Organisaatiossa on valittu yleiseksi ICT-palveluiden toipumisstrategiaksi varalaitteiden käyttö. Tämän vuoksi on olemassa suunnitelmat, miten tärkeimmät palvelut voidaan siirtää olemassa olevaan varalaitteeseen jos tilanne niin vaatii.
Apuvälineitä ja malleja	Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007) • Toipumissuunnitelman runko s. 91 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004) • Luvut 4.3, 5.7 ja 10.6: Eri tyyppisten järjestelmien toipumisen erityispiirteitä Valtionhallinnon ICT-varautumisen esitutkimus Huoltovarmuuskeskuksen jatkuvuuden hallinnan apuvälineet
Huomioita	Organisaatioiden ydinprosessien ja toimivuuden jatkuvuudesta varmistuminen on käsitelty Liitteessä 1 osiossa "Erityistilanteiden hallinta". Tässä käsitellään ainoastaan ICT-järjestelmien toipumista erilaisista häiriöistä ja ongelmista.

2.13 Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta

Osa-alueen nimi	2.13 Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta
Tavoitteet	Kehitettävien ja ylläpidettävien tietojärjestelmien vastaavuus haluttuun tietoturvallisuuden tasoon varmistetaan, riippumatta järjestelmän kehitystavasta (esim. valmisohjelmisto, räätälöity ohjelmisto tai oman kehityksen tulos).
Perustason vaatimukset	1. Järjestelmän omistaja hyväksyy, mitä tietoturvallisuustasoa järjestelmän tulee valmiina tai muutosten jälkeen noudattaa. 2. Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan. 3. Järjestelmän toimivuus testataan ennen tuotantokäyttöön ottamista.
Korotetun tason lisävaatimukset	4. Hankkivalla organisaatiolla on tietoturvavaatimuksia sisältävä tietojärjestelmien arkkitehtuurilinjaus, jonka mukaisia hankittavien tai kehitettävien järjestelmien tulee olla. 5. Jos organisaatio hankkii räätälöityjä tietojärjestelmiä tai kehittää niitä itse, organisaatiolla on dokumentoitu tietojärjestelmän kehitysprosessi, jonka eri vaiheissa on otettu tietoturvallisuus huomioon. 6. Osana hankinta- tai kehitysprojektia järjestelmästä valmistuu kirjallinen turvallisuussuunnitelma ja käyttäjän ohje, joissa kerrotaan miten järjestelmä suojataan tuotantokäytössä ja millaiset ovat käyttäjiltä vaadittavat tietoturvatoimenpiteet. 7. Järjestelmän määritykset ja toteutukset on auditoitu tietoturvallisuuden osalta
Korkean tason lisävaatimukset	8. Tietoturvavastaava tarkastaa järjestelmän tietoturvakuvauksen, -suunnitelman tai -suunnitelmat. 9. Kehitys- tai räätälöintityön aikana järjestetään katselmointeja tietoturvallisuuden kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja.
Käytännön esimerkkejä	• Vaatimukseen 1: Organisaatiossa on järjestelmien omistajien hyväksymä järjestelmien tärkeysluokitus, jonka perusteella vaadittava tietoturvallisuustaso määräytyy. • Vaatimukseen 2: Riskianalyysin lisäksi VAHTI 5/2004 -ohjeen luvun 10.3 sisältöä käytetään tarkistuslistana hankittavan ohjelmiston tietoturvavaatimusten laadinnassa. • Vaatimukseen 9: Katselmointeja järjestetään esimerkiksi työparikatselmointeina, projektiryhmän tai ohjelmointitiimin kokouksissa tai ulkopuolisen auditoijan tekeminä.
Apuvälineitä ja malleja	Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus (VAHTI 3/2000) Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004) • Luku 10: Ohjelmistoturvallisuus • Sovellusylläpitoon myös luku 12.4: Muutoshallinta Muutos ja tietoturvallisuus, alueellistamisesta ulkoistukseen – Hallittu prosessi (VAHTI 7/2006) • Ulkoistettavan tietojärjestelmän tietoturvallisuuden arviointimalli, s. 61
Huomioita	Tietojärjestelmien hankinnan ja kehityksen hyvät tietoturvallisuuden huomioon ottavat toimintatavat auttavat organisaation kokonais-tietoturvallisuuden varmistamisessa. Mitä aikaisemmin hankinta- tai kehitysvaiheissa ohjelmistolle asetettavat tietoturvavaatimukset ovat tiedossa, sitä laadukkaampaa on jälki ja sitä pienemmät ovat kustannukset. Tietoturvavaatimusten laadinnassa riskianalyysi on hyvä keino, kunhan analyysissä keskitytään itse järjestelmään eikä projektin aikataulu- ja henkilöriskeihin. Erityisesti tarjouspyyntövaiheessa on syytä olla mahdollisimman tarkat vaatimukset tietoturvallisuudelle, jotta tietoturvallisuus tulisi otettua huomioon mahdollisimman aikaisessa vaiheessa. Yksi parhaita ohjelmointityön laatuun positiivisesti vaikuttavia keinoja on katselmointien järjestäminen ja kehittäjien tietoisuus katselmoinneista.

Liite 6. Korvaava menettely

On mahdollista, että organisaatio ei toimintansa erityispiirteistä johtuvasta hyvästä syystä pysty toteuttamaan yksittäisiä tietoturvallisuustasojen asettamia vaatimuksia. Tällöin on mahdollista ottaa käyttöön korvaavia menettelytapoja , joiden avulla vaatimusten alkuperäinen tavoite saadaan kuitenkin täytettyä ja riittävä tietoturvallisuuden taso varmistettua. Korvaavia menet-telyjä voidaan käyttää väliaikaisesti esimerkiksi silloin, kun alkuperäisen vaatimuksen toteuttaminen on budjetissa sijoitettu vasta TTS-suunnitte-lujakson loppupuolelle. Esim. yksittäistä järjestelmää koskeva tekninen rajoitus ei kuitenkaan ole riittävä peruste vaatimuksesta poikkeamiseen kaikkien järjestelmien kohdalla.

Huomattavaa on, että lakisääteisille vaatimuksille ei voida käyttää korvaavia menettelytapoja.

Edellytyksenä korvaavan menettelytavan hyväksymiselle on, että organisaatio on dokumentoinut riittävät perustelut alkuperäisestä vaatimuksesta poikkeamiselle, arvioinut poikkeamisesta aiheutuvat riskit, sekä määritellyt ja toteuttanut riittävät menettelyt riskin pienentämiseksi alkuperäisen vaatimuksen tarkoittamalle tasolle. Organisaation johdon on nämä perustelut hyväksyttävä.

Useiden organisaatioiden toimintaa koskevien tietojenkäsittely-ympäristöjen osalta pelkkä organisaation sisäinen hyväksyntä ei riitä, vaan korvaavan menettelyn käytön hyväksyy aina ulkopuolinen auditoija, joka on valtiovarainministeriön hyväksymä. Korvaavien menettelyjen käyttöä tulee välttää, ne ovat aina yksittäistapauksia ja niiden lukumäärä tulee minimoida.

Jokaisesta korvaavasta menettelystä on täytettävä alla oleva kuvaus:

Korvaavan menettelyn kuvaus

Korvattava vaatimus	Nimeä tähän alkuperäinen vaatimus, jota korvaava menettely koskee.
Perustelu, miksi vaatimusta ei voida täyttää	Kuvaa perustelut, miksi organisaation on mahdotonta toteuttaa alkuperäistä vaatimusta.
Vaatimuksen tavoite ja riskiarvio	Kuvaa alkuperäisen vaatimuksen tavoite tai riski, jonka hallitsemiseksi alkuperäinen vaatimus on olemassa, sekä vaatimuksesta poikkeamisesta aiheutuva riski.
Korvaavan menettelyn kuvaus	Kuvaa vaihtoehtoinen tapa tai tavat, joilla alkuperäisen vaatimuksen tavoite organisaatiossa täytetään tai vaatimuksesta poikkeamisen aiheuttama riski pienennetään vaatimuksen toteuttamista vastaavalle tai sitä paremmalle tasolle.
Korvaavan menettelyn voimassaoloaika	Korvaavat menettelyt on pääasiassa tarkoitettu väliaikaisiksi ratkaisuiksi. Anna aikataulu, jonka puitteissa alkuperäinen vaatimus on tarkoitus toteuttaa.
Hyväksynnät	Korvaavien menettelyjen käytön edellytys on, että vähintään organisaation johto on ne katselmoinut sekä todennut ne tarpeellisiksi ja riittäviksi.

Liite 7. Voimassaolevia VAHTI-julkaisuja

- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010
- VAHTIn toimintakertomus vuodelta 2009, VAHTI 1/2010
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä, VAHTI 7/2009
- Kohdistetut hyökkäykset, VAHTI 6/2009
- Effective Information Security, VAHTI 5/2009
- Information Security Instructions for Personnel, VAHTI 4/2009
- Lokiohje, VAHTI 3/2009
- ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, VAHTI 2/2009
- VAHTIn toimintakertomus vuodelta 2008, VAHTI 1/2009
- Hankkeen tietoturvaohje, VAHTI 9/2008
- Valtionhallinnon tietoturvasanasto, VAHTI 8/2008
- Informationssäkerhetsanvisning för personalen, VAHTI 7/2008
- Tietoturvallisuus on asenne- Selvitys julkishallinnon tietoturvakoulutustarpeista, VAHTI 6/2008
- Valtion ympärivuorokautisen tietoturvatoiminnan hanke-esitys, VAHTI 5/2008
- Valtionhallinnon salauskäytäntöjen tietoturvaohje VAHTI 3/2008
- Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- VAHTIn toimintakertomus vuodelta 2007, VAHTI 1/2008
- Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007
- Älypuhelimien tietoturvallisuus - hyvät käytännöt, VAHTI 2/2007
- Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007
- Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006
- Tietoturvakouluttajan opas, VAHTI 11/2006
- Henkilöstön tietoturvaohje, VAHTI 10/2006
- Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006

- Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006
- Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006
- Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006
- Selvitys valtion ympärivuorokautisen tietoturvatoiminnan järjestämisestä, VAHTI 4/2006
- Selvitys valtionhallinnon tietoturvaresurssien jakamisesta, VAHTI 3/2006
- Electronic Mail-handling Instruction for State Government, VAHTI 2/2006
- Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005
- Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005
- Information Security and management by Results, VAHTI 1/2005
- Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004
- Datasäkerhet och resultatstyrning, VAHTI 4/2004
- Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004
- Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
- Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
- Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin 09 160 01
Telefaksi 09 160 33123
www.vm.fi

2/2010
VAHTI
lokakuu 2010

ISSN 1455-2566 (nid.)
ISBN 978-952-251-125-6 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-124-9 (pdf)