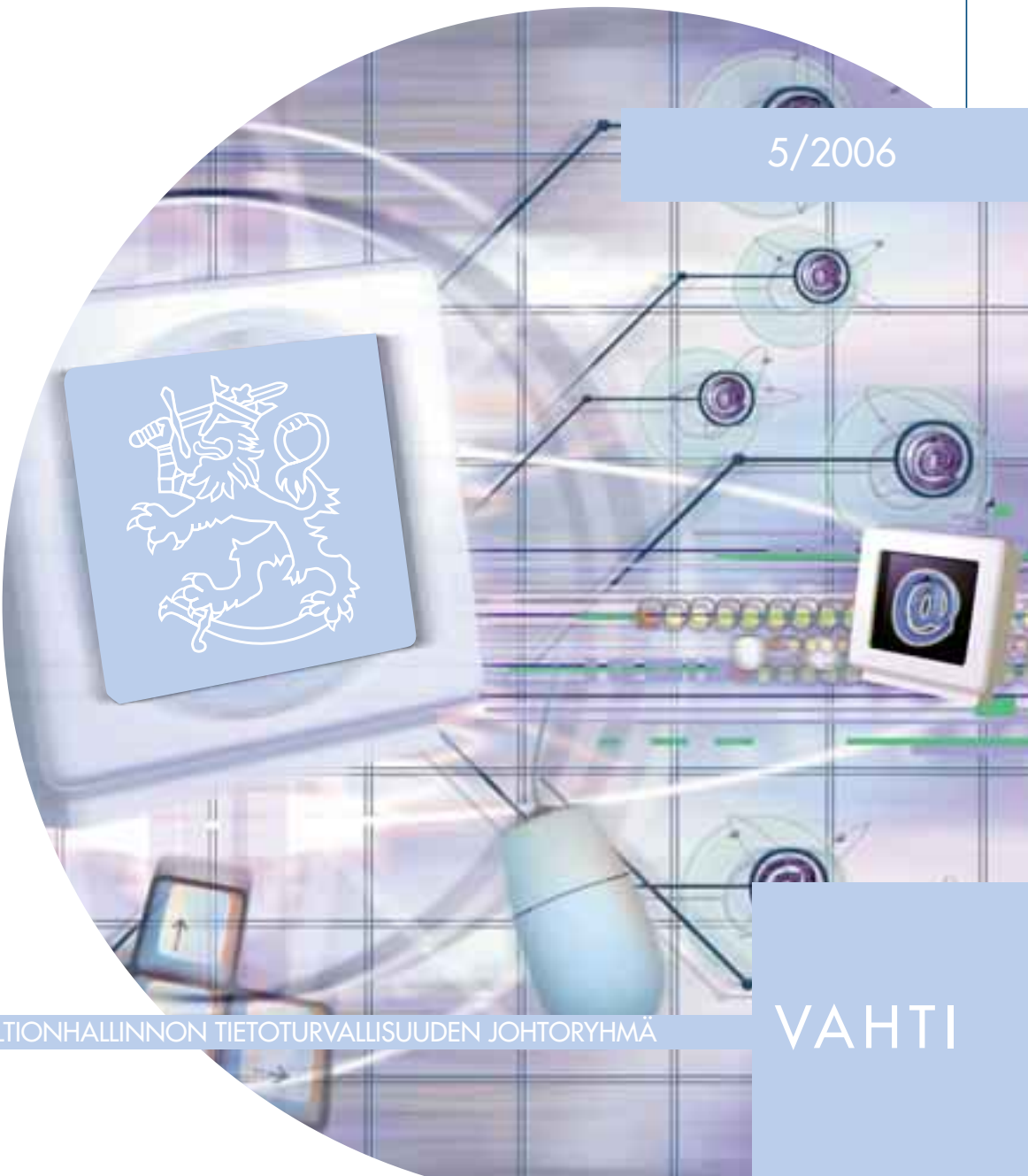
VALTIOVARAINMINISTERIÖ

ASIANHALLINNAN TIETOTURVALLISUUTTA KOSKEVA OHJE



5/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

ASIANHALLINNAN TIETOTURVALLISUUTTA KOSKEVA OHJE

5/2006

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33104

ISSN 1455-2566
ISBN 951-804-611-5 (nid.)
ISBN 951-804-612-3 (pdf)

Edita Prima Oy
HELSINKI 2006

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 15/01/2006

OHJE
29.5.2006

Ministeriöille, virastoille ja laitoksille

ASIANHALLINNAN TIETOTURVALLISUUTTA KOSKEVA OHJE

Valtiovarainministeriö antaa oheisen tietoturvaohjeen (jäljempänä ohje), joka on laadittu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta.

Ohje on tarkoitettu organisaation johdolle sekä asiakirjahallinnon suunnittelu- ja kehittämistehtävissä ja tietohallinto- ja tietoturvatehtävissä toimiville. Ohje täydentää laajaa olemassa olevaa valtion VAHTI-tietoturvaohjeistoa.

Asiakirjalliset tiedot ovat osa organisaation pääomaa ja niiden laatuvaatimukset on turvattava, käsittelykäytännöt suunniteltava huolellisesti ja suojaaminen varmistettava. Asiakirjallisten tietojen hallintaan ja laatuun liittyvien vaatimusten toteuttaminen on suurelta osin tietoturvallisuudesta huolehtimista.

Valtionhallinnon organisaatioiden on toiminnassaan edistettävä asianhallinnan tietoturvallisuutta tukevan toimintakulttuurin luomista sekä jatkuvaa kehittämistä ja ylläpitämistä. Johdon tehtävänä on määritellä asianhallinnan tavoitetila sekä huolehtia asianhallinnan tietoturvallisuuden varmistamisesta, kehittämisestä ja seurannasta.

Ohje tulee VAHTIn Internet-sivuille (www.vm.fi/vahti). Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää (etunimi.sukunimi@vm.fi) ja neuvotteleva virkamies, VAHTIn puheenjohtaja Mikael Kiviniemi (etunimi.sukunimi@vm.fi)

Toinen valtiovarainministeri Ulla-Maj Wideroos

Neuvotteleva virkamies Mikael Kiviniemi

Liite *Asianhallinnan tietoturvallisuutta koskeva ohje (VAHTI 5/2006)*

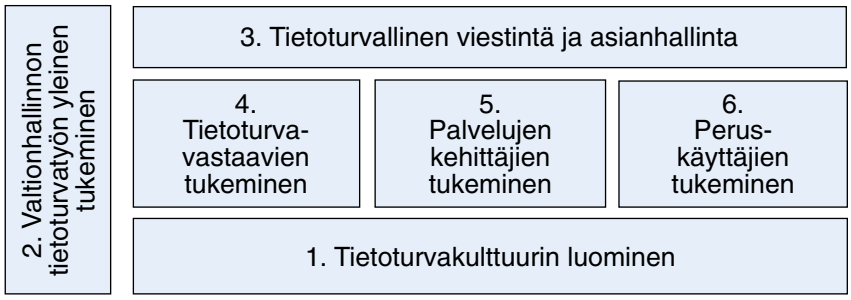
ESIPUHE

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on tunnettu muun muassa tietoturvajulkaisuista ja -ohjeista sekä tietoturvahankkeistaan (www.vm.fi/vahti).

Valtion tietoturvallisuuden kehitysohjelma on julkaistu VAHTI-julkaisusarjassa nimellä *Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006*, VAHTI 1/2004. Kehitysohjelmalla kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Kehitysohjelmaan sisältyy kaikkiaan 28 laajaa kehittämiskohdetta, joista osaa toimeenpannaan työryhmien tai jaostojen valmistelussa ja osaa muilla toimenpiteillä.

Kehitysohjelmaan osallistuvat laajasti kaikki hallinnonalat ja lisäksi osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä ulkopuolisia asiantuntijoita. Hankkeissa on vuonna 2005 ollut mukana valtionhallintotasolla nimettyinä noin 300 osallistujaa. Osa kehitysohjelman kehitystyöstä toteutetaan hanketyöllä ja osa muulla ohjaus-, kehitys- ja yhteistyöllä. Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä (http://www.hare.vn.f/) VAHTIn (VM166:00/2003) alahankkeina. Seuraavassa kuvassa on esitettyinä kehitysohjelman osa-alueet.



Tämä asiakirjan on laatinut VAHTIn alainen asianhallinnan tietoturvallisuus- työryhmä. Työryhmän työ on osa kehitysohjelman tietoturvallinen viestintä ja asianhallinta- hankealuetta.

VAHTIn toiminnan kokonaisuutta vuodelta 2005 on kuvattuna VAHTIn toiminta-kertomuksessa (VAHTI 1/2006).

Sisällysluettelo

TIIVISTELMÄ ORGANISAATION JOHDOLLE

Organisaatioiden on toiminnassaan edistettävä asianhallinnan tietoturvallisuutta tukevan toimintakulttuurin luomista ja ylläpitämistä. Tämä edellyttää johdon tukea, riittäviä resursseja, henkilöstön koulutusta, ohjeiden jatkuvaa ylläpitoa sekä valvontaa ja seurantaa. Organisaation johto vastaa toiminnan tietoturvallisuudesta ja tietoturvapolitiikan määrittelemisestä. Johdon tehtävänä on myös määritellä asianhallinnan tavoitetila.

Asianhallinta tarkoittaa organisaation toimintaprosesseihin sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista ja arkistointia sekä asiakirjallisten tietojen hallintaa.

Tämä asianhallinnan ja sitä tukevien tietojärjestelmien tietoturvallisuuden edistämistä käsittelevä ohje on tarkoitettu julkishallinnon organisaatioiden asiakirjahallinnon suunnittelu- ja kehittämistehtävissä sekä tietohallinnossa toimiville henkilöille.

Asiakirjalliset tiedot ovat osa organisaation pääomaa, jolloin niiden laatuvaatimukset on turvattava, käsittelykäytännöt suunniteltava huolellisesti ja suojaaminen varmistettava. Asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat alkuperäisyyden, eheyden, luotettavuuden ja käytettävyyden takaaminen. Asiakirjallisten tietojen hallintaan ja laatuun liittyvien vaatimusten toteuttaminen on käytännössä pitkälti niiden tietoturvallisuudesta huolehtimista. Nämä vaatimukset sisältyvät myös viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 18 §:ään. Vaatimusten toteuttaminen edellyttää, että

- organisaation toimintaprosessit ja niihin liittyvät tietojen käsittelyprosessit on kuvattu kattavasti koko elinkaaren ajalta ja prosesseille on nimetty omistajat
- prosessien omistajat vastaavat prosessien kehittämisestä sekä tietojen käsittelyyn ja käyttöön liittyvistä menettelytavoista
- organisaatiolla on ajantasaiset tiedot sen tietovarannoista, käsittelemistä asioista ja asioiden käsittelyvaiheista
- tietojärjestelmistä on laadittu kuvaukset ja julkisia kuvauksia pidetään yleisön saatavilla

- tietojärjestelmien määrittely- ja suunnitteluvaiheessa selvitetään niiden tietosisällön julkisuus, salassapito ja suojaaminen
- asiakirjallisen tiedon käsittelijöillä on tarvittava tieto käsiteltävien asioiden julkisuuteen ja salassapitoon, tietojen antamiseen ja suojaamiseen liittyvistä menettelytavoista sekä tietoturvajärjestelyistä
- asiakirjallisia tietoja käsitellään, rekisteröidään ja arkistoidaan asianmukaisesti
- tarpeettomat tiedot ja asiakirjat hävitetään asianmukaisesti tietosuoja huomioon ottaen

1. JOHDANTO

1.1. Asiakirjallisen tiedon laatuvaatimukset

Asiakirjallisilla tiedoilla tarkoitetaan organisaation tehtävien ja toimintojen yhteydessä kertyviä tietoja. Asiakirjallisen tiedon käsite on välineneutraali. Koska asiakirjalliset tiedot dokumentoivat organisaation tehtäviä ja siten tukevat sen toiminnan tavoitteita sekä takaavat toiminnan jatkuvuuden ja jäljitettävyyden, on asiakirjallisten tietojen todistusvoimaisuus kyettävä varmistamaan.

Todistusvoimaisuuden varmistamiseksi asiakirjallisten tietojen käsittelyyn ja hallintaan liittyy erityisvaatimuksia, jotka viranomaisympäristössä on määritelty lainsäädännössä. Viranomaisten asiakirjallisia tietoja koskevat erityisvaatimukset perustuvat julkisuuslainsäädäntöön, arkistolakiin ja henkilötietolakiin, mutta vaatimuksia voi sisältyä myös erityislainsäädäntöön. Mainitussa lainsäädännössä edellytettyjä erityisvaatimuksia ovat tietojen laadun varmistaminen, niiden julkisuuden ja salassapidon toteuttaminen sekä tietojen asianmukainen arkistointi tai hävittäminen.[1]

Asiakirjalliset tiedot ovat osa organisaatioiden pääomaa, jolloin niiden laatuvaatimukset on varmistettava, käsittelykäytännöt suunniteltava huolellisesti ja suojaaminen varmistettava. Siten organisaatioiden toiminnan kannalta on tärkeää, että asiakirjalliset tiedot ovat ajan tasalla, oikeiden henkilöiden saatavilla ja etteivät ne joudu vääriin käsiin.[2] Sivullisia ovat kaikki ne tahot, joille ei ole myönnetty oikeutta käsitellä kyseisiä asiakirjallisia tietoja.[3]

Asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat alkuperäisyyden, eheyden, luotettavuuden ja käytettävyyden takaaminen.

---

[1] Arkistolaki 831/1994; ISO 15489-standardi Information and documentation – Records management – Part 1.

[2] Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003.

[3] Arkaluonteiset kansainväliset tietoaineistot. VAHTI 4/2002.

- Asiakirjallinen tieto on alkuperäistä, kun se on tarkasteluhetkellä sama luotettava todistuskappale kuin valmistumishetkellä. Alkuperäisen asiakirjallisen tiedon laatijan tai lähettäjän identiteetin sekä laatimis- ja lähettämisajankohdan on oltava todennettavissa.
- Asiakirjallisen tiedon eheys varmistetaan turvaamalla tieto valtuudettomilta korjauksilta ja muutoksilta määrittelemällä, mitä täydennyksiä ja lisäyksiä asiakirjalliseen tietoon laatimisen/valmistumisen jälkeen saa tehdä ja millaisissa tilanteissa. Jokainen asiakirjalliseen tietoon tehtävä täydennys, lisäys ja poisto tulisi dokumentoida ja olla jäljitettävissä tekijään.
- Asiakirjallisen tiedon luotettavuuden varmistaminen edellyttää, että asiakirjallinen tieto on laadittu sen tapahtuman yhteydessä, jota se dokumentoi, ja että asiakirjallisen tiedon laatija voidaan todentaa tai että asiakirjallinen tieto on tallennettu niillä järjestelmillä tai välineillä, joita käytetään kyseisessä toiminnassa tai sen toimenpiteen toteuttamisessa, jota asiakirjallinen tieto dokumentoi.
- Asiakirjallisen tiedon käytettävyys varmistetaan, kun tieto on paikallistettavissa, saatavissa esille, esitettävissä ja tulkittavissa. Tulkittavuuden vaatimus täyttyy, kun asiakirjallinen tieto on liitettävissä kontekstiinsa eli niihin tehtäviin ja toimenpiteisiin, joiden tuloksena asiakirjallinen tieto on syntynyt ja joiden yhteydessä sitä on käytetty, sekä muihin asiakirjallisiin tietoihin, jotka ovat syntyneet samojen tehtävien ja toimenpiteiden tuloksena.[4]

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999; julkisuuslaki) 18 §:ään sisältyviä asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat tiedon saatavuuden, käytettävyyden ja eheyden varmistaminen sekä tietojen suojaaminen. Nämä vaatimukset täyttyvät, kun

- organisaatiolla on ajantasaiset kuvaukset omista toimintaprosesseistaan sekä niihin liittyvistä asioiden ja asiakirjojen käsittelykäytännöistä
- organisaatio pitää luetteloa käsiteltäväksi annetuista ja otetuista sekä käsitellyistä ja ratkaistuista asioista
- tietojärjestelmistä on laadittu kuvaukset ja julkisia kuvauksia pidetään yleisön saatavilla
- tietojärjestelmien määrittely- ja suunnitteluvaiheessa selvitetään niiden tietosisällön julkisuus, salassapito ja suojaaminen
- tietojärjestelmät on suunniteltu sellaisiksi, että asiakirjallisten tietojen julkisuus voidaan vaivattomasti toteuttaa ja salassa pidettävät tiedot suojata
- julkiset ja salassa pidettävät tiedot voidaan vaivattomasti erottaa toisistaan
- asiakirjallisen tiedon käsittelijöillä on tarvittava tieto käsiteltävien asiakirjojen julki-

[4] ISO 15489-standardi Information and documentation – Records management – Part 1.

suudesta ja salassapidosta, tietojen antamisesta ja käsittelystä, suojaamisen menettelyistä, tietoturvajärjestelyistä ja tehtävänjaosta
- asiakirjalliset tiedot arkistoidaan asianmukaisesti
- määräajan säilytettävät asiakirjalliset tiedot hävitetään välittömästi niiden säilytysaikojen umpeuduttua

Asiakirjallisten tietojen hallintaan ja laatuun liittyvien vaatimusten toteuttaminen on käytännössä pitkälti niiden tietoturvallisuudesta huolehtimista. Tietoturvallisuus tarkoittaa tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista hallinnollisilla, teknisillä ja muilla toimenpiteillä. Suojaaminen koskee normaalioloja, normaaliolojen häiriötilanteita ja poikkeusoloja. Tietoturvallisuus kytkeytyy kiinteästi organisaation prosessien ja niitä tukevien tietojärjestelmien kehitystyöhön.[5] Käsittelyprosessien suunnittelussa on otettava huomioon kirjausketjut[6], hyväksymismenettelyt ja vaaralliset työyhdistelmät. Samalla määritetään prosesseihin liittyvät kontrollit. Tietoturvallisuus on siten osa organisaation toiminnan ja tietojenkäsittelyn laatua.

Tietoturvallisuus voidaan jakaa hallinnolliseen tietoturvallisuuteen, henkilöstöturvallisuuteen, fyysiseen turvallisuuteen, tietoliikenne-, laitteisto- ja ohjelmistoturvallisuuteen, tietoaineistoturvallisuuteen sekä käyttöturvallisuuteen.[7] Asianhallinnan tietoturvallisuudella on liittymäpintoja jokaiseen toimenpidealueeseen.

Asianhallinta tarkoittaa organisaation toimintaprosesseihin sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista ja arkistointia sekä asiakirjallisten tietojen hallintaa.

Asianhallintajärjestelmä määritellään tietojärjestelmäksi, jonka avulla organisaation käsittelemät asiat ja niihin liittyvät asiakirjat hallitaan ennalta määriteltyjen käsittelysääntöjen mukaisesti. Asiankäsittelyjärjestelmässä on olennaista, että järjestelmään tallennetut tai liitetyt asiakirjat liittyvät aina toimenpiteen/käsittelyvaiheen kautta asiaan. Asiakirjojen kontekstin turvaamisen kautta pystytään takaamaan asiakirjalliseen tietoon kohdistuvat laatuvaatimukset. Ilman asiasidosta järjestelmään tallennettuja asiakirjoja ei voida säilyttää pitkän aikaa yksinomaan sähköisessä muodossa. Dokumenttienhallintajärjestelmien kehittämisessä huomiota on nimenomaan kiinnitettävä siihen, että järjestelmiin tallennettavat asiakirjat voidaan liittää oikeaan kontekstiinsa, osaksi sitä tehtävää, jonka yhteydessä asiakirjat ovat syntyneet.

[5] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

[6] Tietojen käsittely ja katselu on pystyttävä jäljittämään.

[7] Tietoturvakäsitteistö. VAHTI 4/2003.

1.2. Ohjeen tavoite

Tämän ohjeen tavoitteena on edistää organisaatioiden asianhallinnan ja sitä tukevien tietojärjestelmien (asian- ja dokumenttienhallintajärjestelmien ja työryhmäohjelmistojen) tietoturvallisuutta. Ohje on suunnattu julkishallinnon organisaatioiden asiakirjahallinnon suunnittelu- ja kehittämistehtävissä sekä tietohallinnossa toimiville henkilöille.

Tarkoituksena on kiinnittää erityistä huomiota tietoturvaominaisuuksien toteuttamiseen asian- ja dokumenttienhallintajärjestelmien määrittely- ja käyttöönottovaiheessa. Sähköisessä toimintaympäristössä asioiden ja asiakirjallisten tietojen laatuun liittyvät vaatimukset toteutetaan järjestelmän toiminnallisuutena.[8] Toiminnallisuutta toteutetaan pitkälti tietojärjestelmän metatietomäärittelyn avulla. Siksi tässä ohjeessa määritellään myös asianhallinnan tietoturvallisuutta toteuttavat metatiedot. Luotettavan asianhallinnan näkökulmasta on tärkeää, että metatietoarvot tallentuvat tietojärjestelmään mahdollisimman automaattisesti ja että käyttäjät tallentavat metatietoarvoja rajoitetusti.[9]

Tietoturvallisuuteen sisältyy olennaisesti tiedon luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen sekä todentamisen ja kiistämättömyyden varmistaminen.[10] Todentamiseen ja kiistämättömyyteen on kiinnitettävä erityistä huomiota silloin, kun järjestelmän käyttäjät on tunnistettava vuorovaikutteisia sähköisiä asiointipalveluita käytettäessä tai kun organisaation työntekijä etäkäyttää työpaikkansa tietojärjestelmiä. Tässä ohjeessa tarkastellaan näiden tietoturvallisuuden keskeisten osa-alueiden toteuttamista asianhallinnan tietoturvallisuuden näkökulmasta sekä edellä esitettyjen asiakirjallisten tietojen laatuvaatimusten linkittymistä tietoturvallisuuden osa-alueisiin.

Tietoturvavaatimukset koskevat sekä sähköisessä että manuaalisessa muodossa olevan tiedon koko käsittelyprosessia. Sähköiseen toimintaympäristöön siirtymisessä on erityisesti otettava huomioon tietojärjestelmien yhteensopivuus ja turvallisuus. Toimintaprosessien jatkuva sähköistyminen merkitsee sitä, että manuaalisen tietojen käsittelyn tietoturvallisuuden taso täytyy siirtää tietojärjestelmien tietoturvallisuuteen. Toisaalta sähköiseen tietojärjestelmään on helpompi liittää tietoturvallisuutta ohjaavia elementtejä, kuten automaattisesti täydentyviä asian ja asiakirjan käsittelyä ohjaavia metatietoarvoja. Organisaation oman ja sen asiakkaiden oikeusturvan takaamiseksi on huolehdittava julkisuuslain vaatimusten mukaisesti tietojärjestelmien suojaamisesta ja tietojärjestelmien tietosisällön luotettavuudesta, ajantasaisuudesta, oikeellisuudesta, käytettävyydestä ja kattavuudesta.

Tietoaineistoille on laadittava käsittelyohjeet. Aineisto on säilytettävä siten, etteivät tiedot muutu tai häviä asiattomasti. Siten erityisesti pysyvästi ja pitkän aikaa säilytettävien

[8] JHS 143 (www.jhs-suositukset.fi/suomi/jhs143).

[9] Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

[10] Tietoturvallisuuden hallintajärjestelmän arviointisuositus. VAHTI 3/2003.

asiakirjallisten tietojen eheyteen ja käytettävyyden takaamiseen on kiinnitettävä huomiota.

Tietoturvallisuuden toteuttaminen organisaatiossa edellyttää tietoturvaperiaatteiden ja -politiikan määrittelyä, luotettavaa ja koulutettua henkilöstöä, tietojenkäsittely-ympäristön suojaamista, tietoliikenteen salausta ja käytön valvontaa, laitteistojen kunnossapitoa, laadukkaita ja hyvin suunniteltuja ohjelmistoja sekä tietoaineistojen luokittamista ja hallinnoimista. Organisaatioiden on toiminnassaan edistettävä asianhallinnan tietoturvallisuutta tukevan toimintakulttuurin luomista ja ylläpitämistä. Tämä edellyttää johdon tukea, riittäviä resursseja, henkilöstön koulutusta, ohjeiden jatkuvaa ylläpitoa sekä valvontaa ja seurantaa.[11] Organisaation johto vastaa toiminnan tietoturvallisuudesta. Johdon tehtävänä on myös määritellä asianhallinnan tavoitetila.

1.3 Ohjeen laatiminen

Asianhallinnan tietoturvallisuutta koskeva ohje on valmisteltu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI alaisuudessa ja ohjauksessa.

Ohjeen on laatinut kehittämispäällikkö Päivi Happonen Kansallisarkistosta. Ohjeen tietosisällön suunnitteluun on osallistunut vuonna 2004 perustettu VAHTIn asianhallinnan tietoturvatyöryhmä.

Työryhmään ovat kuuluneet

Juhani Tikkanen, Kansallisarkisto, puheenjohtaja (2004–2005)
Jaana Kilkki, Sota-arkisto (2004–2005)
Iris Karhuketo, oikeusministeriö (2005)
Juhani Koivunen, valtiovarainministeriö (2004)
Petri Konttinen, maa- ja metsätalousministeriön tietopalvelukeskus (2004–2005)
Jukka Korhonen, teknillinen korkeakoulu (2004–2005)
Heli Lehtinen, verohallitus (2004–2005)
Jukka Leino, oikeusministeriö (2004)
Anna-Maija Marttila, valtiovarainministeriö (2004–2005)
Anne Miettinen, liikenne- ja viestintäministeriö (2004–2005)
Sauli Santikko, suojelupoliisi (2004–2005)
Minna Saros, Pirkanmaan ympäristökeskus (2004–2005)
Päivi Tommila, kauppa- ja teollisuusministeriö (2004–2005)
Päivi Happonen, Kansallisarkisto, sihteeri (2004–2005).

VAHTI ohjasi työtä kokouksissaan. Ohje viimeisteltiin toteutetun laajan lausuntokierroksen ja VAHTIn linjausten pohjalta.

[11] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

2. TOIMINTAPROSESSIEN JA ELINKAAREN SUUNNITTELUN MERKITYS

Asianhallinnan tietoturvallisuuden kehittämisen ensimmäinen askel on organisaation toimintaprosessien kuvaaminen. Prosesseja kuvattaessa käydään läpi, miten asiat tulevat vireille, miten asian käsittely organisaatiossa etenee, miten asiat päätetään sekä mitä rooleja (osallistujia) prosessien eri vaiheisiin liittyy. Samalla määritellään prosessien omistajat, mikä selkiyttää prosesseihin liittyviä vastuukysymyksiä. Omistaja vastaa prosessista kertyvien tietojen käsittelystä ja käytöstä tietojen säilytysmuodosta riippumatta[12].

Selkeät prosessit varmistavat toiminnan laatua ja sujuvuutta. Toimintaprosessien kuvaamisen yhteydessä kartoitetaan mahdollisimman tarkasti myös asiakirjaprosessit (prosessien eri vaiheista kertyvät tiedot) ja asiakirjallisten tietojen käsittelysäännöt (käsittelyvaiheet, tietojen tallentaminen tai rekisteröiminen tietojärjestelmään). Asiakirjaprosessien läpikäynti on osa organisaation tietoriskien hallintaa.[13]

Käsittelykäytäntöjen selvittämisen yhteydessä määritellään asiakirjallisten tietojen ja tietojärjestelmien merkitys organisaation toiminnan kannalta eli tietojen säilytysajat ja määräajan säilytettävien asiakirjallisten tietojen säilytysajan päättymisen laskentaperusteet sekä tietojen hävittämiskäytännöt. Tiedon elinkaaren suunnitteluun kytkeytyy olennaisesti tiedon säilytysmuoto ja siihen mahdollisesti kohdistuvat muutokset: tulostetaanko sähköinen tieto paperille, missä vaiheessa tulostaminen tapahtuu ja kuka siitä vastaa? Pysyvästi säilytettävät tiedot on tulostettava paperille tai mikrofilmille, mikäli organisaatioilla ei ole arkistolaitoksen myöntämää lupaa säilyttää tiettyyn rekisteriin tai tietojärjestelmään sisältyvät pysyvästi säilytettävät tiedot yksinomaan sähköisessä muodossa. Määräajan säilytettävät asiakirjalliset tiedot organisaatio voi säilyttää ainoastaan sähköisessä muodossa, mikäli se pystyy turvaamaan asiakirjallisten tietojen alkuperäisyyden, ehey-

[12] Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje. VAHTI 2/2000.

[13] Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003.

den, luotettavuuden ja käytettävyyden. Myös asiakirjallisen tiedon sähköisen ja manuaalisen version säilyttämiskäytännöt on määriteltävä, jolloin ratkaisevaa on, kumpi versio käsitetään alkuperäiseksi asiakirjaksi. Samalla kartoitetaan asiakirjallisten tietojen julkisuusrakenne ja henkilötietoluonne.[14]

Nämä tiedot merkitään arkistonmuodostussuunnitelmaan, joka on organisaation asiakirjallisten tietojen käsittelyn, rekisteröinnin ja säilyttämisen ohjeisto. Arkistonmuodostussuunnitelma on arkistolain (831/1994) piiriin kuuluville organisaatioille pakollinen. Kansallisarkiston tuottamassa arkistonmuodostussuunnitelman laadintaoppaassa esitetään arkistonmuodostussuunnitelman tietosisältövaatimukset (www.narc.fi/ams-opas). Tietosisällölle asetetut vaatimukset ovat analogisia asiakirjahallinnollisten metatietomääritysten[15] kanssa: arkistonmuodostussuunnitelma tuottaa tietojärjestelmiin asiakirjallisen tiedon hallintaan liittyviä metatietoja. Tällöin arkistonmuodostussuunnitelma koordinoi organisaation aktiiviaikaisten asiakirjallisten tietojen käsittelyä ja hallintaa ja siten mahdollistaa tietojen suunnitelmallisen hallinnan myös sähköisessä muodossa.

Taulukossa 1 on kuvattu yleisen asianhallintaprosessin vaiheet, jossa on otettu huomioon myös asiakirjan elinkaari. Prosessi on jaettu neljään päävaiheeseen. Päävaiheet on jaettu alavaiheisiin, joita kaikkia ei esiinny jokaisessa asiassa. Jokaisen alavaiheen yhteyteen on liitetty tieto alavaiheeseen mahdollisesti liittyvän asiakirjan muodosta[16]. Kuvaus on tehty julkishallinnon organisaatioiden näkökulmasta.

Taulukko 1. Yleinen asianhallintaprosessi[17]

Prosessin päävaiheet	Prosessin alavaiheet	Asiakirjan muoto
Vireille tulo	Asiakirjan saapuminen/laatiminen	Manuaalinen tai sähköinen
	Viestin vastaanotto	Sähköinen
	Vastaanottokuittauksen lähettäminen	Sähköinen
	Viestin avaaminen	Sähköinen
	Alkuperäisyyden ja eheyden tarkastaminen	Sähköinen
	Viestin tekninen muokkaaminen	Sähköinen
	Asiakirjallisen luonteen tarkastaminen	Sähköinen
	Asian avaaminen	Manuaalinen tai sähköinen
	Rekisteröinti tai luokittelu	Manuaalinen tai sähköinen
	Asiakirjan liittäminen tietojärjestelmään	Manuaalinen tai sähköinen
	Tiedottaminen	Manuaalinen tai sähköinen

[14] Arkistonmuodostussuunnitelman laadintaopas (www.narc.fi/ams-opas).

[15] Arkistolaitoksen SÄHKE-hankkeessa määritellyt metatietovaatimukset asiankäsittelyjärjestelmille (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf) ja JHS 143 Asiakirjallisten tietojen kuvailussa ja hallinnassa käytettävät metatiedot (www.jhs-suositukset.fi).

[16] Asiakirjalla ei tässä yhteydessä tarkoiteta prosessin alavaiheen tuloksena syntyvää asiakirjaa, vaan asiakirjaa, joka on alavaiheen kohteena.

Prosessin päävaiheet	Prosessin alavaiheet	Asiakirjan muoto
Käsittely	Asian valmistelu	Manuaalinen tai sähköinen
	Lisätietojen, lausuntojen yms. pyytäminen	Manuaalinen tai sähköinen
	Rekisteröinti tai luokittelu	Manuaalinen tai sähköinen
	Asiakirjan liittäminen tietojärjestelmään	Manuaalinen tai sähköinen
	Lisätietojen, lausuntojen yms. vastaanottaminen	Manuaalinen tai sähköinen
	Viestin vastaanotto	Sähköinen
	Vastaanottokuittauksen lähettäminen	Sähköinen
	Viestin avaaminen	Sähköinen
	Alkuperäisyyden ja eheyden tarkastaminen	Sähköinen
	Viestin tekninen muokkaaminen	Sähköinen
	Rekisteröinti tai luokittelu	Manuaalinen tai sähköinen
	Asiakirjan liittäminen tietojärjestelmään	Manuaalinen tai sähköinen
	Kuuleminen	Manuaalinen tai sähköinen
	Tiedottaminen	Manuaalinen tai sähköinen
Päättäminen	Esittely	Manuaalinen tai sähköinen
	Päätösasiakirjan allekirjoittaminen	Manuaalinen tai sähköinen
	Rekisteröinti tai luokittelu	Manuaalinen tai sähköinen
	Päätöksen tallentaminen päätöstietokantaan	Sähköinen
	Sähköinen tiedoksianto	Sähköinen
	Päätöksen lähettäminen	Manuaalinen tai sähköinen
	Tiedottaminen	Manuaalinen tai sähköinen
Arkistointi	Säilyttäminen	Manuaalinen tai sähköinen
	Tietopalvelu	Manuaalinen tai sähköinen
	Seulonta ja hävittäminen	Manuaalinen tai sähköinen
	Konvertointi	Sähköinen
	Siirto pitkäaikaissäilytykseen	Manuaalinen tai sähköinen

Prosessikuvauksia hyödynnetään sekä tietojärjestelmien määrittelyvaiheessa että asiakirjahallinnollisten ohjausvälineiden kehittämisessä. Prosessikuvausten avulla rakennetaan myös organisaation tehtävien luokittelurunko, johon organisaation arkistonmuodostussuunnitelman tehtäväryhmittely, asianhallintajärjestelmän asiaryhmitys tai muussa tietojärjestelmässä käytettävä luokittelu mahdollisimman pitkälle perustuvat. Asiakirjallisen tiedon hallintavälineissä käytettävä yhdenmukainen ryhmittely mahdollistaa sen, että sähköisessä sovelluksessa ylläpidettävä arkistonmuodostussuunnitelma toimii eri tietojärjestelmiin tallentuvien metatietoarvojen ohjausvälineenä. Tällöin asianhallintaa tukevat metatietoarvot saadaan tietojärjestelmiin automaattisesti.

Tietojärjestelmässä tehtävistä asioiden ja asiakirjojen käsittelyyn liittyvistä toimenpiteistä on tallennuttava kattavat merkinnät. Aukoton käsittelyketju ja automaattiset tilasiir-

[17] Julkisuuslain (621/1999) 13 §:n mukaiset asiakirjapyynnöt ja 16 §:n mukaiset rekistereihin kohdistuvat tietopyynnöt sekä niihin liittyvät organisaation päätökset eivät sisälly asianhallinnan prosessikuvaukseen alavaiheina, vaan tietopyyntöjen käsittely on organisaatioissa oma asianhallinnallinen prosessinsa, jonka käsittely etenee kuvatun mallin mukaisesti.

tymät takaavat omalta osaltaan järjestelmään sisältyvien asioiden ja asiakirjojen luotettavuuden, eheyden ja alkuperäisyyden.

Asianhallintajärjestelmään sisältyvien asioiden ja asiakirjojen sekä dokumenttienhallintajärjes-telmään tallennettavien asiakirjojen tilasiirtymät määritellään prosessikohtaisesti: miten asioiden ja asiakirjojen tilat muuttuvat prosessin edetessä, missä vaiheessa asiakirjaan ei enää voi tehdä muutoksia? Tilasiirtymät automatisoidaan, jolloin prosessiin sisältyvän ennalta määritellyn toiminnallisuuden toteutuminen järjestelmässä muuttaa asian ja asiakirjan tilaa. Esimerkiksi vireillä olevan asian päättäminen muuttaa asian tilan päätetyksi ja asiakirjan allekirjoittaminen asiakirjan tilan valmiiksi, jolloin asiakirjatiedosto lukittuu, eikä sen tietosisältöä enää voi muokata. Valmis asiakirja säilyy lukittuna, vaikka päätetty asia avattaisiin uudelleen. Ainoastaan valmiin asiakirjan elinkaarta ohjaavat metatiedot täydentyvät asiakirjan valmis-tilasta huolimatta.[18]

Asianhallinnan tietoturvallisuutta toteutetaan pitkälti tietojärjestelmien metatietojen avulla. Taulukossa 2 on kuvattu asianhallinnan tietoturvallisuutta toteuttavat metatietoelementit yleisen asianhallintaprosessin päävaiheiden tasolla. Metatietoelementit ja niiden tarkenteet perustuvat arkistolaitoksen SÄHKE-määritykseen ja arkistolaitoksen määräykseen asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttämisestä yksinomaan sähköisessä muodossa. Taulukkoon on merkitty SÄHKE-määritysten mukaiset pakolliset asianhallintajärjestelmiä koskevat asioiden ja asiakirjojen metatietoelementit. Metatietomääritys on sovellettavissa myös dokumenttienhallintajärjestelmiin.

Taulukko 2. Asianhallinnan tietoturvallisuutta toteuttavat metatietoelementit asianhallinta- ja dokumenttienhallintajärjestelmissä

Asianhallinnan tietoturvallisuutta tukevat metatiedot	Asianhallintaprosessin päävaihe			
	Vireille tulo	**Käsittely**	**Päättämi-nen**	Arkistointi
Asiataso				
ID-tunnus (järjestelmä) **• asiaryhmän tunnus (käyttäjä valitsee)**	x			
Tila (järjestelmä)	x	x	x	**x**

[18] Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

Käyttörajoitus (AMS): • julkisuusluokka (AMS) • salassapidon peruste (AMS) • turvallisuusluokka (AMS) • salassapitoaika (AMS) • salassapidon päättymisajankohta (AMS + järjestelmä) • henkilötietoluonne (AMS) • omistaja (järjestelmä + AMS) • käsittelyoikeus (henkilö ja rooli, joilla käsittelyoikeus, käsittelyoikeuksien kuvaus) (AMS + järjestelmä + käyttäjä)	x			
Säilytyshistoria (järjestelmä): • ajankohta (järjestelmä) • tekijä (järjestelmä) • auktorisointi (järjestelmä) • muutoksen tyyppi (järjestelmä) • muutoksen syy (järjestelmä) • kuvaus (järjestelmä)	x	x	x	**x**
Tapahtuma- ja muutosloki (järjestelmä): • ajankohta (järjestelmä) • tekijä (järjestelmä) • tapahtumatyyppi (järjestelmä)	x	x	x	**x**
Sijaintipaikka (AMS): • sijaintipaikkatieto (AMS)	x	x	x	**x**

Asiakirjataso	**Vireille tulo**	**Käsittely**	**Päättäminen**	Arkistointi
Tyyppi (käyttäjä/järjestelmä[1])	x	x	x	
ID-tunnus (järjestelmä)	x	x	x	
Tila (järjestelmä)	x	x	x	**x**
Käyttörajoitus (AMS): • julkisuusluokka (AMS) • salassapidon peruste (AMS) • turvallisuusluokka (AMS) • salassapitoaika (AMS) • salassapidon päättymisajankohta (AMS + järjestelmä) • henkilötietoluonne (AMS) • omistaja (järjestelmä + AMS) • käsittelyoikeus (henkilö ja rooli, joilla käsittelyoikeus, käsittelyoikeuksien kuvaus) (AMS + järjestelmä + käyttäjä)	x	x	x	**x**
Säilytysaika (AMS): säilytysajan pituus (AMS) säilytysajan peruste (AMS) säilytysajan päättymisajankohta (AMS + järjestelmä)	x	x	x	**x**

[19] Pääsääntöisesti käyttäjä valitsee esimerkiksi valintalistasta asiakirjatyypin. Prosessista riippuen asiakirjatyyppi voi tallentua järjestelmästä myös automaattisesti silloin, kun sähköinen asiakirjallinen tieto saapuu oikeanmuotoisena ja kun järjestelmä tunnistaa sen.

Hävitysaika (järjestelmä): • hävitysajankohta (järjestelmä) • hävitystapa (järjestelmä) • hävitysperuste (järjestelmä) • auktorisointi (järjestelmä)				x
Säilytyshistoria (järjestelmä): • ajankohta (järjestelmä) • tekijä (järjestelmä) • auktorisointi (järjestelmä) • muutoksen tyyppi (järjestelmä) • muutoksen syy (järjestelmä) • kuvaus (järjestelmä)	x	x	x	**x**
Tapahtuma- ja muutosloki (järjestelmä): • ajankohta (järjestelmä) • tekijä (järjestelmä) • tapahtumatyyppi (järjestelmä) • selite (järjestelmä)	x	x	x	**x**
Sijaintipaikka (AMS): • sijaintipaikkatieto (AMS)	x	x	x	**x**
Suojeluluokka (AMS)	x	x	x	**x**
Asiakirjan alkuperäisyys ja eheys todettu (järjestelmä + käyttäjä): • tarkastaja (järjestelmä) • aikamääre (järjestelmä) • kuvaus (käyttäjä/järjestelmä)[2]	x	x		
Asiakirjan sähköinen allekirjoitus (käyttäjä/järjestelmä)[3]	x	x	x	

Taulukossa esitettyjen asiakirjatason metatietoelementtien sisältö on yhdenmukainen asiakirjojen kuvailun ja hallinnan metatiedoista annetun julkisen hallinnon suosituksen kanssa (JHS 143), vaikka osa metatietoelementeistä on nimetty mainituissa metatietomäärityksissä eri tavoin. Taulukossa on jokaisen metatietoelementin ja sen tarkenteen kohdalla maininta, tallentuuko metatietoelementin ja tarkenteen arvo asiatasolle ja asiakirjatasolle automaattisesti järjestelmästä tai sen ohjausvälineenä toimivasta arkistonmuodostussuunnitelmasta vai tallentaako arvon järjestelmän käyttäjä.

Luotettavan asianhallinnan näkökulmasta on tärkeää, että suurin osa metatietoarvoista tallentuu järjestelmään automaattisesti. Lisätietoja arkistonmuodostussuunnitelman integroinnista tietojärjestelmien taustajärjestelmäksi saa arkistolaitoksen SÄHKE-hankkeen toiminnallisista vaatimuksista sekä vuoden 2006 alussa julkaistusta arkistolaitoksen määräyksestä asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttämisestä yksinomaan sähköisessä muodossa.

[20] Alkuperäisyyttä ja eheyttä koskeva kuvaus voi tallentua automaattisesti järjestelmän tuottamana metatietoarvona tai käyttäjän tallentamana metatietoarvona.

[21] Katso edellinen viite.

3. SALASSA PIDETTÄVIEN TIETOJEN KÄSITTELYKÄYTÄNNÖT

Julkisuuslainsäädännön mukaan tieto on salassa pidettävää ainoastaan julkisuus- ja salassapitosäädösten mukaisesti, muutoin se on julkista. On huomattava, että tieto voi olla myös julkisuus- ja salassapitolainsäädännön ulkopuolella olevaa tietoa. Prosessien ja käsittelykäytäntöjen kartoittamisen yhteydessä käydään läpi organisaatioiden asiakirjallisten tietojen julkisuus- ja salassapitorakenne sekä henkilötietoluonne, jotka merkitään arkistonmuodostussuunnitelmaan. Salassa pidettävistä tai salassa pidettävää tietoa sisältävistä asiakirjallisista tiedoista määritellään arkistonmuodostussuunnitelmaan salassapidon peruste, salassapitoaika, salassapitoajan päättymisen laskentaperuste ja mahdollinen turvallisuusluokka.[22]

Salassa pidettävä tieto on joko turvallisuusluokiteltavaa[23] tai muuta salassa pidettävää tietoa. Turvallisuusluokiteltavat asiakirjat käsittelevät yhteiskunnan turvallisuuden tai tiettyjen keskeisten yleisten etujen vuoksi salassa pidettävää tietoa.[24] Laissa kansainvälisistä tietoturvallisuusvelvoitteista säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi.[25] Salassa pidettävän, turvallisuusluokiteltavan ja arkaluonteisten kansainvälisten tietoaineistojen käsittelystä on annettu omat VAHTI-ohjeensa.

VAHTIn alaisuudessa työskentelee parhaillaan tietoaineistotyöryhmä, jonka työn tuloksena tietoaineistojen luokittelut ja niiden edellyttämät käsittelyvaatimukset tullaan yhtenäistämään siten, että laki-, asetus- ja ohjetasot tukevat toisiaan niin kansallisten kuin

[22] Arkistonmuodostussuunnitelman laadintaopas (www.narc.fi/ams-opas); Arkistolaitoksen SÄHKE-määritykset. Abstrakti mallintaminen (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

[23] Tältä osin ohjeluonnoksessa käytettävä terminologia perustuu luonnokseen valtioneuvoston asetukseksi tietoturvallisuudesta ja hyvästä tiedonhallintatavasta.

[24] Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999).

[25] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004).

kansainvälistenkin aineistojen osalta. Lähtökohtana on nelitasoinen turvallisuus- ja käsittelyluokittelu.

Seuraavassa esitetyt käsittelyn ohjeistamiseen liittyvät suositukset ovat tärkeitä erityisesti asianhallinnan tietoturvallisuuden kannalta.

Salassa pidettävät tiedot on pystyttävä erottamaan julkisista tiedoista. Julkisuuslain mukaan asiakirjan julkisesta osasta on pyydettäessä pystyttävä antamaan tieto.[26] Salassa pidettävää tietoa sisältävästä sähköisestä asiakirjasta asiakirjan omistaja voi tuottaa julkisen version.[27]

Salassa pitoa koskevan merkinnän tekemistä suositellaan myös muihin salassa pidettäviin tietoihin, mutta se ei ole julkisuuslain mukaan pakollista.28 Salassa pidettävien tietojen antamisesta päättää asiakirjan omistaja (käsittelijä/valmistelija), hänen esimiehensä, organisaation lakimies tai asiakirjahallinnon tehtäviä hoitavat henkilöt. Nämä vastuuhenkilöt nimetään arkistonmuodostussuunnitelmaan.[29]

Asianhallinta- ja dokumenttienhallintajärjestelmissä salassa pidettävät ja turvallisuusluokitellut tiedot osoitetaan metatietojen avulla. Salassapito voi kohdistua asiakirjatiedostojen lisäksi myös metatietoihin, jolloin tietojärjestelmän eri kentät pitää pystyä suojaamaan niin, etteivät muut kuin kyseisiin tietoihin käyttöoikeuden omaavat henkilöt näe kyseisiä tietoja. Mikäli järjestelmän kaikkia metatietokenttiä ei voida teknisesti sulkea, on metatietokenttien täyttäminen ohjeistettava niin, että salassa pidettävät tiedot tallennetaan vain niihin kenttiin, jotka voidaan suojata. Sen sijaan turvallisuusluokkiin I ja II kuuluvat asiakirjalliset tiedot rekisteröidään salaiseen diaariin.

Asiakirjahallinnolliset vaatimukset täyttävässä tietojärjestelmässä salassa pitoa osoittavat metatietoarvot tallentuvat arkistonmuodostussuunnitelmasta sekä asiatasolle että asiakirjatasolle. Siitä huolimatta metatietoarvoja pitää tietojärjestelmässä pystyä muuttamaan, mutta muutosoikeudet on käyttöoikeuksin tarkoin rajattava. Asioiden valmistelijoilla tulee olla oikeus muuttaa arkistonmuodostussuunnitelmasta oletusarvoina tallentuvia asioiden ja asiakirjallisten tietojen julkisuutta ja salassapitoa koskevia metatietoarvoja. Salassa pitoon liittyviin metatietoarvoihin tehtävien muutosten on tallennuttava järjestelmän tapahtuma- ja muutoslokiin.[30]

Tietojärjestelmä laskee automaattisesti salassa pidon päättymisen, kun arkistonmuodostussuunnitelmaan määritelty toiminnallisuus toteutuu tietojärjestelmässä tai kun im-

[26] Laki viranomaisten toiminnan julkisuudesta (621/1999).

[27] Arkistolaitoksen SÄHKE-määritykset. Abstrakti mallintaminen (www.narc.fi/sahke).

[28] Laki viranomaisten toiminnan julkisuudesta (621/1999).

[29] Arkistonmuodostussuunnitelman laadintaopas (www.narc.fi/ams-opas)

[30] Arkistolaitoksen SÄHKE-määritykset. Toiminnalliset vaatimukset (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

pulssina toimiva tieto tallentuu järjestelmään metatietoarvoksi tai käsittelyvaihetiedoksi. Tällaisia impulsseja ovat esimerkiksi asiakirjan päiväys ja asian päättäminen. Siten myös salassa pidettävät tai salassa pidettävää tietoa sisältävät asiat (metatiedot) muuttuvat salassapitoajan päätyttyä julkisiksi. Metatietoelementin arvon muuttumisen vahvistaa tähän valtuutettu henkilö.

Sen sijaan sähköisesti ylläpidetyissä salaisissa diaareissa, joissa toistaiseksi ei edellä mainittuja toiminnallisia vaatimuksia ole toteutettu, salassapitomerkintä poistetaan asiakohtaisesti ja asioiden käyttöoikeudet määritetään uudelleen. Manuaalisesta salaisesta diaarista annetaan julkiseksi muuttuneita diaaritietoja esimerkiksi diaariotteella. Julkisen tiedon antamiskäytännöt salaisesta rekisteristä kuvataan tietojärjestelmäselosteessa. Organisaation on nimettävä salaisen diaarin pitäjät ja pidettävä luetteloa näistä henkilöistä.

Kokouksissa salassa pidettävät asiat esitellään omilla esityslistoillaan, jotka kerätään kokouksen päätyttyä pois. Salaisista asioista kootaan oma pöytäkirja, sillä muussa tapauksessa julkisen pöytäkirjan käyttöä joudutaan rajoittamaan.

Salassa pidettävät asiakirjat ja salassa pidettävää tietoa sisältävät siirrettävät tallennusvälineet säilytetään lukitussa tilassa, jolloin sivulliset eivät pääse niihin käsiksi.[31] Mikäli säilytysyksikkö sisältää salassa pidettävää tietoa, on säilytysyksikköön ja arkistoluetteloon merkittävä, että koteloon tai kansioon sisältyy salassa pidettäviä asiakirjoja.

Kun salassa pidettäviä tietoja sisältäviä asiakirjoja siirretään arkistolaitokseen, on salassapitoa osoittavat merkinnät tehtävä jokaiseen salassa pidettäviä asiakirjoja sisältävään luovutettavaan koteloon, sidokseen tai vastaavaan yksikköön sekä tarvittaessa yksittäiseen asiakirjaan. Osittain salaista asiakirjaa koskevasta merkinnästä on käytävä ilmi, miltä osin asiakirja on salassa pidettävä.[32]

[31] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

[32] Asiakirjojen siirtäminen arkistolaitokseen. Arkistolaitoksen määräys 18.1.2002 KA 284/40/2001 (www.narc.fi/Arkistolaitos/siirto-ohje/siirto-ohje.htm).

4. ASIAKIRJALLISTEN TIETOJEN HÄVITTÄMINEN

Määräajan säilytettävä asiakirjallinen tieto on hävitettävä välittömästi sille vahvistetun säilytysajan umpeuduttua. Hävittäminen toteutetaan joko tuhoamalla asiakirja fyysisesti tai saattamalla se muutoin sellaiseen muotoon, ettei sen sisältämää tietoa enää voida käyttää. Salassa pidettävät manuaaliset asiakirjalliset tiedot on hävitettävä siten, etteivät asiattomat pääse niihin käsiksi. Mikrofilmit silputaan, poltetaan ongelmajätelaitoksessa tai niistä poistetaan hopea erikoisliikkeessä. Hävittämisen hoitaa organisaation siihen oikeuttama henkilö, hävittämisessä käytetään riittävän turvallisia menetelmiä ja se tehdään valvotuissa oloissa.

Vastaavat hävittämisvaatimukset koskevat myös sähköisessä muodossa säilytettävää aineistoa. Sähköinen aineisto tuhotaan esimerkiksi päällekirjoittamalla tai tietoväline tuhoamalla.

Arkistolaitoksen SÄHKE-määritysten mukaisesti toteutettu tietojärjestelmä sisältää hävitystoiminnallisuuden, jolloin määräajan säilytettävät asiakirjalliset tiedot hävitetään järjestelmästä luotettavasti niiden säilytysaikojen umpeuduttua. Järjestelmän tietosisältöön kohdistuvan hävitysesityksen tekeminen on mahdollista vain arkistonhoitajan roolin mukaisin käyttöoikeuksin. Yleisen käytännön mukaisesti hävitysesityksen hyväksyy arkistonhoitajan esimies, josta tallentuu tieto asiakirjan metatietoihin. Asiakirjallisten tietojen metatiedot jäävät järjestelmään ja ne täydentyvät hävittämistä koskevilla tiedoilla.[33]

Tietojen siirtäminen rajallisin käyttöoikeuksin varustettuun passiivikantaan ei ole tietojen hävittämistä.

Tietojärjestelmien toiminnallisuuksiin sisältyy mahdollisuus poistaa asioita, toimenpiteitä ja asiakirjoja silloin, kun asian käsittely on kesken ja kun asiakirjaa ei ole lukittu.

[33] Arkistolaitoksen SÄHKE-määritykset. Abstrakti mallintaminen ja toiminnalliset vaatimukset (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

Tällaiset poisto-oikeudet on syytä tiukasti rajoittaa ainoastaan henkilöille, joilla on kirjaajatason ja pääkäyttäjätason oikeudet järjestelmään. Sen sijaan asiakirjan omistajalla pitää olla oikeus poistaa luonnosasiakirja. Poistoista tallentuu tieto lokimerkintöihin.[34]

[34] Arkistolaitoksen SÄHKE-määritykset. Toiminnalliset vaatimukset (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

5. LOKI- JA MUUTOSHISTORIATIEDOT

Tietoaineistojen käytön seurantaa ja valvontaa varten tietojärjestelmiin on tallennuttava automaattisesti lokitietoja tietojen käsittelyyn liittyvistä tapahtumista.[35] Järjestelmien on kerättävä lokitietoja, jotta tietojärjestelmien ja niiden tietosisällön käytettävyys, eheys ja luottamuksellisuus voidaan turvata ja jotta mahdolliset luvattomat toiminnot voidaan havaita. Myös sähköisten asiointipalvelujen käytöstä, kuten oman asian käsittelyn seurannasta, on tallennuttava lokitietoja. Palvelujärjestelmä huolehtii käyttäjien tunnistamisesta.

Koska arkistonmuodostussuunnitelman on tarkoitus toimia tietojärjestelmien ohjausvälineenä ja metatietoarvojen lähteenä, myös arkistonmuodostussuunnitelmaan tehtävistä muutoksista on tallennettuva loki- ja muutoshistoriatietoja. Tällaisia tapahtumia ovat esimerkiksi ryhmitykseen kohdistuvat muutokset, säilytysaikamuutokset tai julkisuusrakenteeseen kohdistuvat muutokset.[36]

Asianhallinnan tietoturvallisuuden näkökulmasta merkityksellisiä lokitietoja ovat tapahtuma- ja muutoslokit, jotka todentavat järjestelmän tietosisältöön kohdistuvia tapahtumia ja toimenpiteitä. Tapahtuma- ja muutoslokiin tallentuu tieto esimerkiksi asiakirjan allekirjoittamisesta, julkisuusarvon muuttumisesta tai asian ja asiakirjan tilasiirtymästä. Tapahtuma- ja muutoslokiin tallennettavien tapahtumien ja toimenpiteiden määrä määritellään organisaatiokohtaisesti[37].

Lokitietoja on säännönmukaisesti seurattava. Lokijärjestelmä on rakennettava niin, että se hälyttää asiattomista käsittely-yrityksistä.[38]

---

[35] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

[36] Arkistolaitoksen SÄHKE-hanke. Abstrakti mallintaminen (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

[37] JHS 143 (www.jhs-suositukset.fi/suomi/jhs143).

[38] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

Pääsyoikeudet järjestelmän lokitietoihin on määriteltävä valvontakohteiden mukaisesti. Lokitietoja ei saa käyttää profiiliyhteenvetojen tekemiseen[39]. Järjestelmän tietosisältö vaikuttaa siihen, pitääkö lokitietoja pystyä salaamaan. Lokitietojen muuttumattomuus voidaan taata esimerkiksi sähköisellä allekirjoituksella.[40] Lokitiedot voivat sisältää myös sähköisen viestinnän tietosuojalaissa tunnistamistiedoiksi määriteltyjä tietoja, jolloin lokitietojen käytön on oltava hyvin rajoitettua. Tällainen tunnistamistieto on esimerkiksi IP-osoite, josta tietojärjestelmää on käytetty.[41]

Lokitietoja kertyy valtavia määriä, joten seurantaa varten kannattaa rakentaa erillinen sovellus esimerkiksi järjestelmän raportointiominaisuuksia hyödyntäen. Tällöin on mahdollista erilaisin ryhmittelykriteerein seurata ja valvoa järjestelmätapahtumia. Tällaisia ryhmittelykriteereitä ovat vähintään kohde (tapahtumatyyppi), tekijä (käyttäjä) ja tapahtuma-aika.[42]

Lokitietojen säilytysaika määritellään lokin käyttötarkoituksen mukaan. Esimerkiksi arkaluonteisia henkilötietoja sisältävien tietojärjestelmien lokitietoja säilytetään niin kauan kuin rekisteröity voi esittää rikosperusteisia vaatimuksia henkilötietojen käsittelijää tai sivullista vastaan.[43] Lokitietojen säilytysaikaa määriteltäessä on otettava huomioon myös niiden merkitys asiakirjallisen tiedon alkuperäisyyden, eheyden ja luotettavuuden varmistamisessa. Sen takia asianhallintajärjestelmään tallentuvat näitä ominaisuuksia tukevat lokitiedot ovat pakollisia metatietoja, jotka säilytetään niin kauan kuin järjestelmä on organisaatiossa käytössä ja jotka tulevaisuudessa siirretään pysyvästi sähköisessä muodossa säilytettävien asiakirjallisten tietojen mukana arkistolaitoksen vastaanotto- ja palvelujärjestelmään.[44]

[39] Valtionhallinnon sähköpostien käsittelyohje. VAHTI 2/2005.

[40] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

[41] Sähköisen viestinnän tietosuojalaki (516/2004).

[42] Arkistolaitoksen SÄHKE-määritykset. Toiminnalliset vaatimukset (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

[43] Asiaa tietosuojasta 1/2003. Käyttäjälokin tietojen käsittely henkilötietolain mukaan.

[44] JHS 143 (www.jhs-suositukset.fi/suomi/jhs143); Arkistolaitoksen SÄHKE-määritykset. Abstrakti mallintaminen (www.narc.fi/sahke); Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa. Arkistolaitoksen määräys 20.12.2005 KA 1486/40/2005 (www.narc.fi/Arkistolaitos/pdf-ohjeet/akj_maarays.pdf).

6. TIETOJÄRJESTELMIIN KOHDISTUVAT VAATIMUKSET

Tietojärjestelmien on täytettävä luotettavan tietojärjestelmän vaatimukset, jolloin asioiden käsittelyprosessit ovat aukottomia ja niihin liittyvät käsittelyvaiheet ja toimenpiteet rekisteröityvät järjestelmään kattavasti ja automaattisesti. Lisäksi järjestelmän metatietomäärityksen on perustuttava asiahallinnan metatietomalliin. Järjestelmän tuotantoympäristön hallinnan tulee teknisesti taata asiakirjallisten tietojen alkuperäisyys, eheys, luotettavuus ja käytettävyys tietojen koko elinkaaren ajan, vaikka järjestelmästä otetaan käyttöön uusia ohjelmistoversioita tai vaikka järjestelmä siirretään kokonaan uuteen tuotantoympäristöön. Järjestelmäympäristövaatimuksiin sisältyvät myös vikasietoisuus ja järjestelmävirheistä toipuminen.

Tietoturvallisuuden keskeiset osa-alueet ja johdantoluvussa esitetyt asiakirjallisten tietojen laatuvaatimukset[45] on otettava asianhallinta- ja dokumenttienhallintajärjestelmien suunnittelussa ja määrittelyssä huomioon seuraavasti:

- Luotettavuus = asiakirjallisten tietojen ja niiden käsittelyprosessin eheys säilyy. Luotettavuuden takaamisessa on otettava huomioon myös johdantoluvussa esitetyt alkuperäisyyttä ja luotettavuutta koskevat vaatimukset.
- Luottamuksellisuus = organisaation tehtäviin liittyvät turvallisuusluokitellut, muutoin salassa pidettävät ja arkaluonteisia henkilötietoja sisältävät asiakirjalliset tiedot ovat vain niiden käytettävissä, joilla on käyttöoikeudet kyseisiin tietoihin. Käyttäjähallinnasta on saatava tieto toisaalta siitä, mitä oikeuksia henkilöille on myönnetty ja toisaalta siitä, mihin järjestelmän sisältämiin tietoihin käyttöoikeudet kohdistuvat.[46]
- Eheys = asiakirjalliset tiedot ovat oikeita ja ajan tasalla, asiakirjalliset tiedot eivät saa muuttua, hävitä eivätkä vahingoittua virheiden/luvattomien toimenpiteiden seurauksena. Tietojärjestelmissä käsiteltäville tiedoille tulee olla koko niiden elinkaa-

[45] ISO 15489-standardi Information and documentation – Records management – Part 1.

[46] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

ren kattavat käsittelysäännöt. Muutosten on oltava todennettavissa kirjausketjusta.[47] Eheyden varmistamiseen vaikuttavat myös johdantoluvussa esitetyt asiakirjallisten tietojen eheyteen ja luotettavuuteen liittyvät vaatimukset.

- Todennus = varmistetaan, että osapuolet asioivat tarkoitetun tahon kanssa. Asiointipalvelu vaatii molemminpuolista todentamista
- Kiistämättömyys = tiedon lähettäjä tai muu tiedon käsittelyn osapuoli ei voi jälkikäteen kiistää lähettäneensä tietoa tai olleensa osapuolena tapahtumassa. Kiistämättömyyden varmistamiseen kytkeytyy myös johdantoluvussa esitetyt asiakirjallisen tiedon alkuperäisyyttä koskevat vaatimukset.
- Pääsynvalvonta = käyttäjien pääsyä järjestelmään ja sen tietoihin rajoitetaan ja valvotaan
- Saatavuus = asiakirjallisten tietojen tulee olla helposti ja viiveettä niiden käytössä, joille tieto kuuluu. Samalla on huolehdittava, että asiakirjalliset tiedot saadaan teknisesti esille. Saatavuuden turvaamisessa on otettava huomioon asiakirjallisten tietojen käytettävyydelle määritetyt vaatimukset.
- Käytettävyys = asiakirjalliset tiedot säilyvät luotettavina, eheinä ja alkuperäisinä niin kauan kuin niitä arkistonmuodostussuunnitelman mukaan säilytetään. Käytettävyyden varmistamisessa on olennaista tuottaa asiakirjallisten tietojen tunnistamista, sisällönkuvailua, luokittelua ja suhteita muihin asiakirjallisiin tietoihin kuvaavat metatiedot. Käytettävyyden turvaamiseen vaikuttavat myös johdantoluvussa esitetyt asiakirjallisen tietojen käytettävyysvaatimukset.

Sähköisten palvelujen kehittäminen on osa organisaation toiminnan kehittämistä.[48] Sähköpostijärjestelmä tai sähköinen asiointipalvelu eivät ole asianhallintajärjestelmiä, vaan ne on tarkoituksenmukaista liittää osaksi asianhallinta- tai dokumenttienhallintajärjestelmää asiakirjallisten tietojen eheyden ja alkuperäisyyden turvaamiseksi. Sähköpostijärjestelmät eivät myöskään ole sähköisiä arkistoja.

Asiakirjallisten tietojen vastaanotto on dokumentoitava siten, että tietojärjestelmään tallennetaan asiakirjan eheyttä ja alkuperäisyyttä ja mahdollista sähköistä allekirjoitusta todentavat metatietoarvot. Kyseiset metatietoarvot voivat tallentua asianomaisiin metatietokenttiin myös järjestelmän tuottamina. Viestin lähettäjälle lähetetään henkilön lähettämä vastaanottokuittaus, joka ei ole kannanotto asian käsittelyn edellytyksiin tai lopputulokseen eikä myöskään sellaisenaan merkitse sitä, että asia on tullut organisaatiossa vireille.[49]

---

[47] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.

[48] Asiointipalvelujen kehittäminen tieto- ja viestintätekniikan keinoin. Julkisen hallinnon sähköisen asioinnin strategia ja kehittämissuunnitelmia. Työryhmämuistioita 11a/2005. Valtiovarainministeriö hallinnon kehittämisosasto.

[49] Arkistolaitoksen SÄHKE-hanke. Abstrakti mallintaminen (www.narc.fi/sahke); Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003.

Tietojärjestelmien varmuuskopioinnista on huolehdittava. Poistettavista tietojärjestelmistä ja niiden osista laaditaan lopettamissuunnitelma, jossa määritellään tietoaineistojen ja ohjelmistojen arkistointi- ja hävittämismenettelyt.

7. KÄYTTÄJÄHALLINTA

Tietojärjestelmässä on oltava luotettava käyttäjähallinta, jolloin ainoastaan auktorisoidut henkilöt pääsevät luomaan, lisäämään, muuttamaan tai poistamaan tietojärjestelmään tai arkistonmuodostussuunnitelmaan sisältyviä tietoja tai tietojen luokitteluperusteita, kuten asiaryhmitystä.

Käyttövaltuudet tarkoittavat tietojärjestelmien käyttäjille myönnettyjä yksilöityjä oikeuksia tietojärjestelmän käyttöön tai tietojen saantiin. Käyttövaltuudet vastaavat työtehtäviä ja ne on pidettävä ajan tasalla. Käyttövaltuuksien antaminen, muuttaminen ja poistaminen on dokumentoitava ja niiden hallinnasta on tallennuttava tietojärjestelmään valvontalokitietoa.

Tietojärjestelmien käyttäjät yksilöidään käyttäjätunnuksen ja todennetaan esimerkiksi salasanan tai virkakortin avulla. Kun tietojärjestelmään kirjaudutaan etäyhteydellä, on edellytettävä luotettavaa tunnistamista.[50] Ulkopuolisten pääsy järjestelmään estetään normaaleilla käyttöoikeuksien hallintamenetelmillä ja palomuuriratkaisuilla.

Organisaation asiakirjallisten tietojen ja tietojärjestelmien on täytettävä edellisessä luvussa määritellyt laatuvaatimukset. Siten asiakirjallisten tietojen käyttöoikeudet on tarkoin määriteltävä. Käyttöoikeusmäärittely tehdään yleensä prosessikohtaisesti. Jatkossa tietojärjestelmiin tallennettavien ja rekisteröitävien asiakirjallisten tietojen käyttöoikeusmäärittelyjen ohjaustiedot on tarkoituksenmukaista tallentaa sähköisesti ylläpidettävään arkistonmuodostussuunnitelmaan, joka toimii tietojärjestelmien ohjaustietokantana. Käyttöoikeusmäärittelyt tehdään arkistonmuodostussuunnitelmaan käyttäjäryhmittäin, jolloin prosesseittain tai jopa asiakirjatyypeittäin määritellään, millä käyttäjäryhmällä on oikeudet kyseiseen prosessiin liittyviin asiakirjallisiin tietoihin tai tietystä prosessista kertyvään tiettyyn asiakirjaan. Sen sijaan käyttäjäryhmiin kuuluvat henkilöt määritellään tietojärjestelmän käyttäjähallinnassa.

[50] Valtionhallinnon etätyön tietoturvallisuusohje. VAHTI 3/2002.

8. TIETOSUOJA OSANA TIETOTURVALLISUUTTA

Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.[51] Tietoturvallisuuden vaarantuessa vaarantuu myös tietosuoja.

Henkilötietolaki (523/1999) edellyttää henkilötietojen käsittelyn suunnittelua, millä on selkeä liittymäpinta asianhallinnan suunnitteluun ja kehittämiseen. Henkilötietolaissa puhutaan hyvästä tietojenkäsittelytavasta, johon sisältyvät henkilötietojen käsittelyä, tietojen laatua, arkaluonteisten henkilötietojen käsittelyä sekä tietoturvallisuutta koskevat periaatteet. Siten hyvää tietojenkäsittelytapaa voidaan pitää osana hyvää tiedonhallintatapaa. Hyvän tiedonhallintatavan näkökulmasta tärkeää on henkilötietojen suojaaminen, henkilötietojen käsittelyn etukäteissuunnittelu, säilytysarvon määrittely sekä tarpeettomaksi käyneiden henkilötietojen hävittäminen.[52]

Organisaation asiakirjallisten tietojen henkilötietoluonne ja henkilötietojen käsittelyprosessit selvitetään samalla, kun käydään läpi asioiden ja asiakirjallisten tietojen käsittelyvaiheita asianhallinnan kehittämisen näkökulmasta (kts. edellä toimintaprosessien ja elinkaaren suunnittelun merkitys). Arkistonmuodostussuunnitelmaan merkitään prosesseittain jokaisen asian ja siihen liittyvän asiakirjatyypin kohdalle, sisältääkö asia ja asiakirja henkilötietoja vai ei. Henkilötietoluonne on asianhallinnan metatietomallissa pakollinen metatietoarvo, joka tallentuu tietojärjestelmään arkistonmuodostussuunnitelmasta.[53] Arkistonmuodostussuunnitelmasta tallentuva metatietoarvo on ohjeellinen, joka on määriteltyjen käyttöoikeuksien mukaisesti tietojärjestelmässä tapauskohtaisesti muutettavissa.

Organisaatioiden henkilörekistereitä koskevissa erillislaeissa on säädetty myös tietojen käsittelyyn ja suojaamiseen liittyvistä periaatteista.

---

[51] Valtionhallinnon tietoturvakäsitteistö. VAHTI 4/2003.

[52] Henkilötietolaki 523/1999; Arkistonmuodostussuunnitelman laadintaopas (www.narc.fi/ams-opas).

[53] Arkistonmuodostussuunnitelman laadintaopas (www.narc.fi/ams-opas); Arkistolaitoksen SÄHKE-hanke; Abstrakti mallintaminen (www.narc.fi/sahke); JHS 143 (www.jhs-suositukset.fi).

Henkilötietojen siirrossa on huolehdittava tiedon salassa pysymisestä ja muuttumattomuudesta.

Internetissä voidaan julkaista ainoastaan julkisia tietoja, joista henkilötiedot on karsittu pois tai joista ei voi muodostaa henkilörekisteriä. Tämä vaatimus on otettava huomioon, kun asianhallinta- ja dokumenttienhallintajärjestelmästä tai muusta tietojärjestelmä tuotetaan käsittelyprosessin aikana tai sen päätyttyä julkaistava versio. Vaatimus koskee myös rekistereitä, joista muodostetaan julkinen versio.

9. ASIANHALLINNAN TIETOTURVALLISUUDEN TARKISTUSLISTA

Vaatimus	Toteuttamistapa
Asiakirjallisten tietojen käsittelykäytännöt	• Kuvataan toimintaprosessit ja käsittelyvaiheet • Kuvataan asiakirjallisen tiedon elinkaari • Määritellään asioiden ja asiakirjojen tilasiirtymät prosesseittain • Määritellään asioiden ja asiakirjojen käyttöoikeudet prosesseittain • Nimetään prosessien omistajat.
Salassa pidettävän aineiston määrittely ja käsittelyn ohjeistaminen	• Määritellään arkistonmuodostussuunnitelmaan määritellään asiakirjallisten tietojen julkisuus/salassapito, salassa pidettävien tietojen salassapitoaika, mahdollinen turvallisuusluokka, salassapitoperuste, salassapidon päättymisen laskeva toiminnallisuus ja henkilötietoluonne • Arkistonmuodostussuunnitelma tuottaa näitä metatietoarvoja tietojärjestelmiin automaattisesti • Laaditaan henkilökunnalle ohjeet salassa pidettävien tietojen ja henkilötietojen käsittelystä niiden luomisesta/vastaanottamisesta hävittämiseen/pysyvään säilytykseen • Ohjeet ovat ajan tasalla ja niitä noudatetaan käytännössä
Asiakirjallisten tietojen hävittäminen	• Hävitetään asiakirjalliset tiedot niiden säilytysaikojen umpeuduttua niin, etteivät ne joudu ulkopuolisten käsiin • Hävitetään manuaaliset asiakirjat silppuria käyttäen tai tekemällä hävittämissopimus hävittämistä harjoittavan yhteisön kanssa • Hävittämissopimukseen sisältyy yhteisön antama sitoumus • Sähköisiin tietojärjestelmiin sisältyvät tiedot hävitetään niiden säilytysaikojen umpeuduttua • Tietojärjestelmiin sisältyvien määräajan säilytettävien tietojen hävittämistä tehostetaan kehittämällä järjestelmien hävittämistoiminnallisuuksia (www.narc.fi/sahke). • Varmuusnauhoilta ja suojakopioilta tietoja ei erikseen hävitetä, vaan ne poistuvat normaalin mediakierron kautta.
Lokitiedot	• Valvotaan tietojärjestelmien käyttöä • Järjestelmä tuottaa lokitietoa käytöstä ja ylläpidosta • Lokitietoja seurataan
Muutosten hallinta ja versiointi	• Metatietoihin ja asiakirjatiedostoihin kohdistuneet muutokset tallentuvat loki- ja muutoshistoriatietoihin suunnitellusti • Kun asiakirjallista tietoa muokataan ja muokattu tiedosto tallennetaan, syntyy asiakirjasta uusi versio • Vain viimeisin versio on muokattavissa

Tietojärjestelmäselosteiden laadinta	• Laaditaan julkisuuslainsäädännön edellyttämä seloste organisaation ylläpitämistä tietojärjestelmistä (selosteen yksityiskohtainen tietosisältö on määritelty valtiovarainministeriön laatimassa tietojärjestelmäselosteen laadintasuosituksessa VM 7/01/2000). • Laaditaan seloste myös niistä tietojärjestelmistä, joissa käsitellään sekä julkista että salassa pidettävää tietoa • Laaditaan myös henkilötietolain mukainen rekisteriseloste, kun järjestelmissä tai rekistereissä käsitellään henkilötietoja
Käyttäjähallinta	• Käyttäjätietoja hallitaan ajantasaisesti ja mahdollisimman keskitetysti • Käyttöoikeudet annetaan käyttäjäryhmille ja ne vastaavat työtehtäviä • Käyttöoikeuksiin kohdistuvista muutoksista tallentuu järjestelmään lokitietoa

LIITE 1 VOIMASSA OLEVA VAHTI OHJEISTUS JA -JULKAISUT

VAHTI 5/2006: Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006: Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006: Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006: Electronic-mail Handling Instruction for State Government
VAHTI 1/2006: VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005: Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005: Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005: Information Security and Management by Results
VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004: Datasäkerhet och resultatstyrning
VAHTI 3/2004: Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004: Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004: Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 6/2003: Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 5/2003: Käyttäjän tietoturvaohje
Datasäkerhetsanvisning för användaren
User's Information Security Instruction
VAHTI 4/2003: Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointi
VAHTI 2/2003: Turvallisen etäkäytön arkkitehtuuri
VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002: Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002: Etätyön tietoturvaohje
VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001: Tietotekniikkahankintojen tietoturvallisuustarkistuslista

VAHTI 4/2001: Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000: Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000: Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)
VAHTI 2/1999: Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti ja ohjeita saa myös tilattua hyvin edullisesti painotalo Editasta.

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

5/2006

ASIANHALLINNAN TIETOTURVALLISUUTTA KOSKEVA OHJE

ISBN 951-804-611-5 (nid.)
ISBN 951-804-612-3 (PDF)
ISSN 1455-2566