VALTIOVARAINMINISTERIÖ

Suunnitelma

2.6.2015

VAHTI

VALTIONHALLINNON TIETO- JA KYBERTURVALLISUUDEN JOHTORYHMÄ

TOIMINTASUUNNITELMA VUOSILLE 2015 - 2016

Hyväksytty VAHTIn kokouksessa 2.6.2015

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

SISÄLLYSLUETTELO

1 VAHTIn toiminnan lähtökohdat

Tietoturva- ja kyberuhkien lisääntyessä ja niiden ollessa entistä haasteellisempia, on suunnitelmallisesti parannettava tietoturva-, kyberturvallisuus- ja varautumistyötä sekä johtamista. Osa julkishallinnon toimijoista on vahvasti panostanut tietoturvallisuuden kehittämiseen, mutta osa ei ole saanut kehitettyä riittävästi tietoturvallisuutta toiminnoissaan tai järjestelmissään.

Valtiovarainministeriö vastaa julkisen hallinnon tieto- ja viestintäteknisten toimintojen (ICT) ohjaamisesta ja kehittämisestä. ICT:llä tarkoitetaan tieto- ja viestintäteknistä toimintaa laajassa merkityksessä kattaen mm. tietohallinnon, arkkitehtuurin, tietojärjestelmät, tietoverkot, tietovarannot, tietotekniikan ja sen hyödyntämisen, tietoturvallisuuden, laitetilat, ICT- palvelut, menetelmät ja ratkaisut sekä tämän toiminnan ohjaamisen, johtamisen, rakenteet, hankehallinnan, säädökset ja varautumisen häiriötilanteisiin ja poikkeusoloihin.

Valtiovarainministeriössä julkisen hallinnon ICT:n ohjauksesta ja kehittämisestä vastaavana organisaationa on Julkisen hallinnon tieto- ja viestintätekninen toiminto (JulkICT), joka toimii ministeriön ylimmän johdon välittömässä alaisuudessa. Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011) korostaa valtiovarainministeriön roolia ja vastuuta koko julkisen hallinnon ICT:n ohjaajana. Tieto- ja kyberturvallisuuden ohjauksesta ministeriötasolla ei Suomessa ole kattavaa lainsäädäntöä. Tässä hajautetussa työnjaossa korostuu VAHTI:n merkitys yhteistyön tehostajana.

Valtioneuvosto teki 26.11.2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätöksellä ohjataan valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa. Periaatepäätöksellä ohjataan valtionhallinnon tietoturvallisuuden kokonaisuutta ja sen keskeisiä liittymäpintoja sidosryhmiin sekä vahvistetaan tietoturvayhteistyötä. Tietoturvallisuuden kehittämisen painopisteitä ovat johtaminen, kokonaisvaltaisuus ja läpäisy, ennaltaehkäisy ja varautuminen sekä tiedon ja sen arvon suojaaminen.

Periaatepäätöksen ja valtioneuvoston ohjesäännön mukaisesti valtiovarainministeriö (VM) ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tieto- ja kyberturvallisuuden kehittämistä sekä asettaa ja ylläpitää toimialallaan yhteistyön ohjaamiseen, kehittämiseen ja koordinaation toimielimet. VM:n asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI on hallinnon tieto- ja kyberturvallisuuden ohjaamisen, kehittämisen, valmistelun ja koordinaation toimielin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuuden linjaukset. Valtion tietoturvallisuutta koskevan periaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTIssa koordinoitavaan yhteistyöhön. Suomen kyberturvallisuustrategia korostaa VAHTIn roolia.

Useat valtiotason linjaukset lisäävät VM:n tehtäviä julkisen hallinnon ICT:n ohjauksessa. Laki julkisen hallinnon tietohallinnon ohjauksesta (2011), Valmiuslaki (2011), tietoturvallisuuden arviointilait (2011), Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (2013), Laki julkisen hallinnon turvallisuusverkkotoiminnasta (2015), yhteiskunnan turvallisuusstrategia (2010) ja valtioneuvoston periaatepäätös valtion tietoturvallisuuden kehittämisestä (2009) korostavat VM:n roolia julkishallinnon ICT:n ja tietoturvallisuuden ohjaajana. Nämä muutokset lisäävät osaltaan VM:n ja VAHTI:n tehtäviä. VM hyödyntää tarvittavin osin VAHTI:a tämän ohjauksen tukena.

VAHTI:n toiminnassa otetaan huomioon hallituksen ohjelma ja laaja-alaiset uudistuskohteet. VAHTI:n toiminnassa ovat aktiivisesti mukana kaikki hallinnonalat, kunnallishallinto ja yliopistot.

VAHTI:n toiminnalla parannetaan valtion tieto- ja kyberturvallisuutta, ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä sekä kansainvälisesti. Tuloksena on saatu aikaan yksi maailman kattavimmista yleisistä tietoturvaohjeistoista (www.vm.fi/vahti ja www.vahtiohje.fi). VM:n ja VAHTI:n johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita sekä laaja valtion tietoturvallisuuden kehitysohjelma. VAHTI on saanut kolme kertaa tunnustuspalkinnon toiminnastaan Suomen tietoturvallisuuden parantamisessa.

1.1 VAHTI:n tavoitteet

VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä julkisen hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTI:n tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä tietosuojan huomioon ottamista. Tavoitteena on lisäksi edistää tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista, tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja tieto- ja viestintäteknisten palvelujen kehittämistä, ylläpitoa ja käyttöä.

VAHTI edistää hallitusohjelman, yhteiskunnan turvallisuusstrategian, Suomen kyberturvallisuusstrategian, julkisen hallinnon ICT-strategian, valtionhallinnon tietoturvallisuutta koskevan valtioneuvoston periaatepäätöksen ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä julkisen hallinnon ja erityisesti valtionhallinnon tieto- ja kyberturvallisuutta sekä näihin liittyvää yhteistyötä.

1.2 VAHTI:n tehtävät

VAHTI on julkisen hallinnon tietoturvallisuuden kehittämisen, ohjauksen ja yhteistyön toimielin. VAHTI käsittelee julkisen hallinnon tieto- ja kyberturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tieto- ja kyberturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI edistää verkostomaisen toimintatavan kehittämistä julkisen hallinnon tietoturvatyössä.

Lisäksi VAHTI:

- Valmistelee ja yhteensovittaa valtioneuvoston ja valtiovarainministeriön linjauksia julkisen hallinnon tieto- ja kyberturvallisuudesta ja ICT-varautumisesta sekä seuraa ja edistää niiden toimeenpanoa.
- Kehittää, yhteensovittaa ja ylläpitää julkisen hallinnon tieto- ja kyberturvallisuuden tavoitteita, toiminta-, organisointi-, arkkitehtuuri- ja resurssilinjauksia sekä normeja, ohjeita ja suosituksia.
- Edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta.
- Käsittelee ja yhteensovittaa julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia ja vaikuttamista kansainvälisessä tietoturvatyössä.
- Ohjaa ja käsittelee julkisen hallinnon ICT-strategiaa sekä sen valmistelua ja toimeenpanoa tieto- ja kyberturvallisuuden ja ICT-varautumisen osalta.

- Ohjaa, valmistelee ja yhteensovittaa julkisen hallinnon tieto- ja kyberturvallisuuteen liittyviä kehittämisohjelmia ja niiden toimeenpanoa.

Kyberturvallisuusstrategian mukaan VAHTI käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuutta koskevat asiat.

VAHTI osallistuu tarvittaessa valtionhallinnon näkökulmasta kansallista ja kansainvälistä tietoturvallisuutta kehittävien yhteistyöryhmien toimintaan sekä valmistelee tai valmisteluttaa näiden kanssa mahdollisesti valtionhallinnolle annettavat linjaukset tai muut yhteistyöelimen tehtävään sisältyvät valtion tietoturvallisuuteen liittyvät asiat. VAHTI myös tarvittaessa osallistuu, nimeää edustajansa tai antaa asiantuntijatukea hallinnon laaja-alaisiin kehittämishankkeisiin tietoturvallisuuden varmistamiseksi ja integroimiseksi osaksi kehityshankkeiden toimintaa.

2 Valtionhallinnon tietoturvallisuuden kehittämistoimet 2015 – 2016

VAHTI:n toiminta on laaja-alaista ja keinovalikoimaltaan monipuolista. Seuraavissa kappaleissa kuvataan tehtäväalueita yleisellä tasolla. Tähän suunnitelmaan ei ole sisällytetty yksittäisiä toimenpiteitä eikä hankkeiden tarkempaa sisältöä.

2.1 Säädösten ja valtioneuvoston periaatepäätösten toimeenpano ja valmistelu

VAHTI ohjaa valtion tietoturvallisuuden kehittämistä ja tarvittavia hankkeita, kuten korotetun tietoturvatason ja ICT-varautumisen yhteishanketta.

VAHTI osallistuu ja tukee tietoturvallisuuslainsäädännön kehittämistä osana vireillä olevan tiedonhallinnan ja tietojenkäsittelyä koskevan yleislain valmistelua. VAHTI tarvittaessa käynnistää ja osallistuu toimenpiteisiin ICT-varautumisen ja kyberturvallisuuden lainsäädännön ja valtioneuvoston periaatepäätösten kehittämistarpeiden selvittämiseksi.

VAHTI tukee VM:ää Valtorin, Viestintäviraston, Huoltovarmuuskeskuksen, Suomen turvallisuusverkko oy:n ja HALTIK:n tuottamien valtionhallinnon yhteisten tietoturvapalveluiden ohjauksessa. VAHTI ohjaa ja seuraa yhteisten tietoturvapalveluiden ja -ratkaisujen käyttöä sekä tietoturvallisuuden suunnitelmallista sisällyttämistä kehittämishankkeisiin.

VAHTI tekninen jaosto tukee ICT-teknistä turvallisuustyötä ja hankintojen ohjausta. VAHTI tukee tarvittaessa valtiojohtoa tieto- ja kyberturvallisuuden rakenteiden kehittämisessä.

VAHTI valmistelee toimintakertomuksen, johon sisältyy linjausten toteutumisen, VAHTI-toiminnan sekä valtion tieto- ja kyberturvallisuustilanteen kuvaus. Viranomaisyhteistyössä kehitetään toimintatapoja hallinnonalojen varojen ja resurssien kohdentamisessa VAHTI:n koordinoimaan yhteistyöhön.

Valtionhallinnon tietoturvallisuuden toimeenpanossa vastuu kansainvälisten erityissuojattavien tietoaineistojen osalta on kansallisella turvallisuusviranomaisella, NSA:lla.

VAHTI tarvittaessa käynnistää ja osallistuu toimenpiteisiin ICT-varautumisen sekä tieto- ja kyberturvallisuuden lainsäädännön ja valtioneuvoston periaatepäätösten kehittämistarpeiden selvittämiseksi.

2.2 Yhteistoiminta, viestintä, verkostot ja seminaarit

VAHTI toimii aktiivisessa yhteistoiminnassa hallinnonalojen, virastojen ja tietoturvatoimijoiden sekä eritoten valtioneuvoston periaatepäätöksessä 26.11.2009 sekä kyberturvallisuusstrategiassa 24.1.2013 linjattujen yhteiskunnallisten toimijoiden kanssa. Näitä toimijoita ovat VAHTI:n lisäksi kaikki ministeriöt, Viestintävirasto, Valtiokonttori, Valtori, Arkistolaitos, Huoltovarmuuskeskus, Puolustusvoimat, Suomen kuntaliitto, Tietosuojavaltuutetun toimisto sekä valtioneuvoston hallintoyksikön, sisäministeriön ja puolustushallinnon hallinnonalan tietoturvapalveluja tuottavat organisaatiot.

VAHTI kehittää yhteistyötään mm. turvallisuuskomitean, kansallisen turvallisuusviranomaisen (NSA), ministeriöiden valmiusvastaavien sekä julkisen hallinnon kokonaisarkkitehtuurista vastaavien kanssa. Jokainen VAHTI:n jäsen sekä sihteeristön jäsen viestii aktiivisesti VAHTI:sta, sekä sen tuloksista ja toiminnasta. VAHTI ja sen alaryhmät järjestävät tieto- ja kyberturvallisuusseminaareja ajankohtaisista teemoista.

VAHTI valmistelee julkisen hallinnon tieto- ja kyberturvallisuuden vaatimusten ja linjausten kokonaisuuden kuvauksen.

VAHTI:n aineistoja hyödynnetään monipuolisesti ja sen toimintaa esitellään laajasti julkishallinnossa. VAHTI kehittää toimintamalleja tieto- ja kyberturvallisuuden ottamiseksi huomioon JulkICT-toiminnon hankkeissa ja julkisen hallinnon kokonaisarkkitehtuurin kehittämisessä. VAHTI seuraa ja osaltaan osallistuu hallinnon turvallisuusverkkotoiminnan (TUVE) ja yhteisen salausratkaisun (SATU) sekä tarvittaessa muiden palveluiden tieto- ja kyberturvallisuuden ohjaukseen.

2.3 VAHTI-ohjeiston ja julkaisujen kehittäminen

VAHTI-ohjeiston kattavuudesta, sisällöstä ja laadusta huolehtiminen on keskeinen tehtävä. jonka hoitamiseksi on perustettu VAHTI:n ohjejaosto. Se arvioi ohjeiden kehittämistarpeita ja tekee tarvittaessa esityksiä hankkeista ohjeiston kehittämiseksi.

Toimikauden aikana toteutettavat VAHTI-ohjeiden ja julkaisujen kehittämishankkeet ovat:

- Salausohje
- Tietoturvapoikkeamien hallinta
- Toiminnan jatkuvuuden hallinta
- Sähköinen asiointi
- Keskeisten tietojärjestelmien turvaaminen
- Etätyö ja etäkäyttö
- Riskienhallinta
- Tieto- ja kyberturvallisuussanasto

VAHTI ja sen ohjejaosto voivat tarvittaessa käynnistää muitakin ohjeiston kehittämishankkeita.

VAHTI-ohjeiston hyödyntämisen tehostamiseksi VM huolehtii rakenteistetun, sähköisen VAHTI-ohjeiston ensimmäisen version (https://www.vahtiohje.fi) ylläpidosta ja sen

sisällön ajantasaisuudesta. VAHTI suunnittelee ja käynnistää toteuttamisen sähköisen VAHTI-ohjeiston kehittämis- ja ylläpitoprosessille vuonna 2016.

Osana kunkin ohjeen valmistelua, ohjeryhmä suunnittelee sen jalkauttamisen. Ohjeiston kehittämisessä otetaan huomioon VAHTI:n vastuu julkisen hallinnon kyberturvallisuuden linjaamisessa.

2.4 Kyberturvallisuusstrategian toimeenpano

Kyberturvallisuusstrategiassa on annettu VAHTI:lle tehtäviä. Strategian toimeenpano-ohjelmassa on esitetty VAHTI:lle toimenpiteitä liittyen ICT-varautumiseen, kuntien tieto- ja kyberturvallisuuteen sekä osaamisen kehittämiseen. VAHTI valmistelee ja toteuttaa toimenpiteet tarvittavassa laajuudessa.

Hallinnonaloilla on merkittäviä tehtäviä ja vastuita kyberturvallisuusstrategian toimeenpanossa. VAHTI:ssa käsitellään ja seurataan toimenpiteiden kokonaisuutta ja hallinnonalojen tilannetta. VAHTI panostaa tiiviiseen yhteistyöhön Turvallisuuskomitean kanssa.

Kyberturvallisuusstrategian mukaisesti VAHTI käsittelee kaikki merkittävät valtionhallinnon kyberturvallisuutta koskevat asiat. Kyberturvallisuuskeskuksen toimeenpanoon ja ohjaukseen liittyen VAHTI käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset.

2.5 Tieto- ja kyberturvallisuusosaamisen kehittäminen

VAHTI kehittää tieto- ja kyberturvallisuusosaamista ohjaamalla julkisen hallinnon tietoturvallisuuden koulutustoimintaa. VAHTI:n tavoitteena on aktiivisella yhteistoiminnalla, verkostoitumisella, aktiivisella viestinnällä sekä koulutus- ja seminaaritoiminnalla parantaa tieto- ja kyberturvallisuustietoisuutta ja edistää VAHTI-ohjeiden käyttöä.

VAHTI yhteistyössä vastuuvirastojen kanssa tuottaa ja kehittää olemassa olevia verkkokoulutuksia, joiden kohderyhminä ovat ensisijaisesti organisaatioiden johto, henkilöstö ja turvallisuuden vastuuhenkilöt.

VAHTI käynnistää toimenpiteitä, joiden tarkoituksena on laajentaa valtionhallinnon johdon ja henkilökunnan osallistumista tietoturvallisuuden verkkokoulutuksiin ja tenttien suorittamiseen.

2.6 Seuranta, tilannekuva ja arviointi

VM ja VAHTI seuraavat tieto- ja kyberturvallisuuden kehittymistä hallinnon toimijoille tehtävillä kyselyillä, jotka ovat osa valtion tieto- ja kyberturvallisuuden tilannekuvan ylläpitoa. VAHTI kehittää jatkuvasti tieto- ja kyberturvallisuuden sekä ICT-varautumisen mittaamista ja hyödyntää kyselyiden tuloksia ja tehtyjä johtopäätöksiä toiminnan suunnittelussa jatkuvan kehittämisen periaatteiden mukaisesti. Mittariston kehittämisessä otetaan huomioon valtiojohdon tarpeet ja keskeiset strategiat. VAHTI:n mittariston käyttöä laajennetaan kattamaan Suomen koko julkishallinto.

VAHTI ohjaa ja kehittää valtion tietoturva-arviointitoimintaa. Osana sitä VAHTI käsittelee Viestintäviraston tietoturvallisuuden arviointitoiminnan kohteiden valintaa sekä tarkastuksia.

2.7 Tietoturvallisuuden häiriötilanteiden hallinta ja tilannekuva valtiohallinnossa

VAHTI tukee VM:ää SecICT-hankkeen ohjauksessa. Hankkeen tavoitteena on parantaa valtion kykyä ennaltaehkäistä ja hoitaa vakavia sekä laajavaikutteisia tieto- ja kyberhäiriötilanteita.

Vuoden 2015 keskeisenä painopisteenä on valtion yhteisen tieto- ja kyberturvallisuuden tilannekuvaympäristön suunnittelu, laajavaikutteisten tieto- ja kyberhäiriötilanteiden hallintaan tarvittavan toimijaverkoston kokoaminen sekä viranomaisten häiriönhallintayhteistyön kehittäminen.

Hankkeessa jatketaan Viestintäviraston GovCERT- ja GovHAVARO-palveluiden hyödyntämistä ja häiriönhallintatoiminnan ja yhteistyön (VIRT) kehittämistä. Hankkeen tarkoituksena on kehittää häiriönhallinnan pikaviestintäjärjestelmä sekä valmistella tilannekuvajärjestelmän hankinta. Hanke päättyy vuoden 2015 loppuun mennessä, jolloin suunnitellut palvelut siirtyvät tuotantotoiminnaksi.

2.8 Julkishallinnon tieto- ja kyberturvallisuus

VAHTI edistää VAHTI:n ohjeiden käyttöä ja verkostomaista tietoturvayhteistyötä hyödynnettäväksi nykyistä laajemmin koko julkishallinnossa ja sen käyttämissä ja tuottamissa palveluissa.

VAHTI:n perustama kuntien tietoturvajaosto tukee toiminnallaan VM:ä, VAHTI:a ja kuntia tieto- ja kyberturvallisuuteen liittyvässä kehittämisessä ja sen valmistelussa.

VAHTI:n tavoitteena on varmistaa tieto- ja kyberturvallisuuden näkökulman riittävän vahva sisällyttäminen merkittäviin kehittämishankkeisiin, kuten Kansallisen palveluarkkitehtuurin kehittäminen ja uuden hallitusohjelman julkishallinnon uudistushankkeet.

2.9 Kansainvälinen toiminta

VAHTI vaikuttaa kansainvälisessä tietoturvayhteistyössä kattaen esimerkiksi OECD-yhteistyö, EU-yhteistyö, ENISAn toiminta ja tietosuojaviranomaisten yhteistyö. VAHTI:n verkostomaista toimintaa ja yhteistyötä kehitetään kansainvälisen tietoturvayhteistyön sekä kansainvälisten tietoturvavelvoitteiden ja NSA-toimintojen osalta. Kansainvälisiin tietoturvavelvoitteisiin liittyvien asioiden osalta panostetaan erityisesti yhteistyöhön NSAn kanssa.

VAHTI-julkaisuja käännetään ruotsiksi ja englanniksi tehtäviin nimettyjen ohjausryhmien avulla. Jatketaan VAHTI-esitysten pitämistä ja VAHTI:n käännettyjen aineistojen hyödyntämistä.

Selvitetään hallinnon toimijoiden osallistumista kansainväliseen tieto- ja kyberturvallisuuden yhteistyöhön sekä valmistellaan tarvittavia kehittämistoimia.

Liite 1 Voimassa olevia VAHTI-julkaisuja

VAHTI 2/2014 Tietoturvallisuuden arviointiohje
VAHTI 1/2014 VAHTIn toimintakertomus 2013
VAHTI 5/2013 Päätelaitteiden tietoturvaohje
VAHTI 4/2013 Henkilöstön tietoturvaohje
VAHTI 4b/2013 Personnel Information Security Instructions
VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
VAHTI 3/2012 Teknisen ICT-ympäristön tietoturvataso-ohje
VAHTI 2/2012 ICT-varautumisen vaatimukset (uudistettavana)
VAHTI 2b/2012 Requirements for ICT Contingency Planning
VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011 Johdon tietoturvaopas
VAHTI 4/2010 Sosiaalisen median tietoturvaohje
VAHTI 3/2010 Sisäverkko-ohje
VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 2b/2010 Instructions on Implementing the Decree on Information Security in Central Government
VAHTI 2c/2010 Anvisning om verkställighet av förordningen om informationssäkeheten inom statsförvaltningen
VAHTI 7/2009 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009 Kohdistetut hyökkäykset (uudistettavana)
VAHTI 5/2009 Effective Information Security
VAHTI 3/2009 Lokiohje
VAHTI 2/2009 ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin (uudistettavana)
VAHTI 9/2008 Hankkeen tietoturvaohje
VAHTI 8/2008 Valtionhallinnon tietoturvasanasto
VAHTI 7/2008 Informationssäkerhetsanvisningar för personalen (uudistettavana)
VAHTI 6/2008 Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008 Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys
VAHTI 4/2008 Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008 Valtionhallinnon salauskäytäntöjen tietoturvaohje (uudistettavana)
VAHTI 2/2008 Tärkein tekijä on ihminen – Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007 Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 1/2007 Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006 Tunnistaminen julkishallinnon verkkopalveluissa (uudistettavana)
VAHTI 11/2006 Tietoturvakouluttajan opas
VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
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 3/2005 Tietoturvapoikkeamatilanteiden hallinta (uudistettavana)
VAHTI 2/2005 Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005 Information Security and Management by Results
VAHTI 5/2004 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (uudistettavana)
VAHTI 4/2004 Datasäkerhet och resultatstyrning
VAHTI 3/2004 Haittaohjelmilta suojautumisen yleisohje (uudistettavana)
VAHTI 2/2004 Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003 Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002 Valtionhallinnon etätyön tietoturvaohje
VAHTI 4/2001 Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje (uudistettavana)

*Ohjeisto on VAHTIn verkkosivuilla **www.vm.fi/vahti** ja rakenteistetun VAHTI-ohjeiston ensimmäisessä versiossa www.vahtiohje.fi.*