VALTIOVARAINMINISTERIÖ

Johdon tieto-turva-opas

2/2011 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Johdon tietoturvaopas

Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2011 VAHTI

Painotuote

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 978-952-251-279-6 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-280-2 (PDF)

Juvenes Print
Tampereen Yliopistopaino Oy, 2011

VALTIOVARAINMINISTERIÖ

Julkisen hallinnon ICT-toiminto

VM/1980/00.00.00/2011
OHJE
2.12.2011

Ministeriöille, virastoille ja laitoksille

JOHDON TIETOTURVAOPAS

Johdon tietoturvaopas (VAHTI 2/2011) on tarkoitettu valtionhallinnon organisaatioiden johto- ja esimiesasemassa oleville henkilöille. Opas kertoo organisaation tietoturvallisuudesta ja tietoturvavelvoitteista sekä vastaa kysymykseen, miksi tietoturvallisuutta tulisi toteuttaa.

Valtioneuvoston periaatepäätöksessä valtionhallinnon tietoturvallisuuden kehittämisestä (26.11.2009) yhdeksi tietoturvallisuuden kehittämisen painopisteeksi linjataan johtaminen. Oppaan avulla tuetaan valtionhallinnon johtajia ja esimiehiä tietoturvallisuuden sisällyttämisessä organisaation johtamiseen.

Organisaation tietoturvatyön perustaksi tarvitaan näkyvä johdon tuki, jolla varmistetaan työn toteuttamisen edellytykset. Tietoturvallisuuden tulee olla kiinteä osa organisaation johtamista ja toiminnan suunnittelua. Johdon tulee osoittaa tietoturvatyölle resurssit ja ohjausmekanismit organisaation tavoitteiden toteuttamiseksi.

Johdon tietoturvavelvoitteet kuvataan lainmukaisuuden, riskienhallinnan, tietoturvallisuuden johtamisen, organisoinnin, suunnittelun, poikkeama- ja erityistilanteiden hallinnan sekä raportoinnin, tietoturvallisuuden perustason ja toiminnan laatuun nivomisen kannalta.

Opas kuvaa tietoturvallisuuden johtamista lähinnä perustason kannalta. Valtionhallinnon tietoturvallisuusasetuksen (681/2010) mukaisesti jokaisen valtion organisaation on aikaansaatava tietoturvallisuuden perustaso syyskuun 2013 loppuun mennessä. Opas tukee osaltaan virastojen johtoa tässä pakollisessa ja useimmille organisaatioille tietoturvallisuuden kehittämistä edellyttävässä tehtävässä.

Hallinto- ja kuntaministeri — Henna Virkkunen

Valtion IT-johtaja — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: *Johdon tietoturvaopas (VAHTI 2/2011)*

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

Puh 09 160 01 tai 09 578 11 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

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, valtionhallinnon tietoturvallisuusasetuksen (681/2010), Yhteiskunnan turvallisuusstrategian (YTS), 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. Periaatepäätöksen 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 ja www.vahtiohje.fi). 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 tietoturvallisuuden johtamiseen

Johdon tietoturvaopas on valtionhallinnon organisaatioiden johto- ja esimiesasemassa oleville henkilöille tarkoitettu tiivis tietoturvajohtamisen käsikirja. Opas kertoo organisaation tietoturvallisuudesta, mitä tietoturvavelvoitteita organisaatiolla on ja miksi tietoturvallisuutta tulisi toteuttaa.

Tietoturvallisuudella suojataan lakiperusteisesti organisaation omaan toimintaan, yhteiskunnan toimintaan sekä kansalaisiin liittyviä tietoja. Oikeat ja luotettavat tiedot ovat keskeinen osa valtionhallinnon organisaatioiden ja yhteiskunnan päätöksentekoa sekä toimintavarmuutta. Tiedoista huolehtiminen on tärkeässä osassa yhteiskunnan toimintojen turvallisuuden ja jatkuvuuden varmistamisessa sekä kansalaisten perusoikeuksien toteutumisessa.

Tietoturvallisuuden organisointi ja toteutus tulee tehdä siten, että se tukee parhaalla mahdollisella, kustannustehokkaalla tavalla organisaation hyvän hallintotavan toteuttamista sekä perustehtävä- ja strategiatavoitteiden saavuttamista. Tietoturvallisuuden toteuttamisessa keskeisiä ovat myös hyvän tiedonhallintatavan velvoitteet, joiden kautta tietoturvallisuudella on tärkeä rooli turvallisen tietoteknisen ympäristön ja tietohallintotoiminnan ylläpitämisessä ja kehittämisessä.

Valtioneuvoston periaatepäätös tietoturvallisuudesta, 26.11.2009

Riittävä tietoturvallisuuden, varautumisen ja suojauksen taso tulee määritellä ja toteuttaa ottaen huomioon asiaa koskevat säädökset ja käyttäen perustana kunkin organisaation toiminnallisia tavoitteita ja toimintojen tietosisällön arvoa ja merkitystä valtionhallinnolle, kansalaisille ja yhteisöille. Säädösten sekä organisaatiokohtaisten tavoitteiden, toimintojen ja tietojen lisäksi riittävän tietoturvallisuuden, varautumisen ja suojauksen tason määrittämisen ja toteuttamisen lähtökohtia ovat valtionvarainministeriön antamat tietoturvallisuuden ja varautumisen tasot ja -ohjeet.

Tietoturvatyön perustaksi tarvitaan näkyvä johdon tuki, jolla varmistetaan työn toteuttamisen edellytykset. Tietoturvallisuuden tulee olla kiinteä osa organisaation johtamista ja toiminnan suunnittelua. Johdon tulee osoittaa tietoturvatyölle riittävät resurssit ja tarvittavat ohjausmekanismit organisaation tietoturvatavoitteiden toteuttamiseksi. Tietoturvallisuuden tavoitteet ja näiden saavuttamiseksi tarvittavat toimenpiteet tulee arvioida riskienhallintaprosessin ja sen perusteella laaditun vuosisuunnittelun pohjalta.

Yhteiskunnan tietoturvariskien hallitsemiseksi ja tietoturvallisuuden kehittämiseksi valtionhallinnossa on 1.10.2010 astunut voimaan Asetus tietoturvallisuudesta valtionhallinnossa 681/2010. Asetus edellyttää viranomaisilta siinä kuvattujen tietoturvallisuuden perustason vaatimusten täyttämistä 30.9.2013 mennessä.

Asetus tietoturvallisuudesta valtionhallinnossa 23§.

Viranomaisen tietojenkäsittely on saatettava vastaamaan asetuksen 5 §:ssä säädettyjä perustason tietoturvallisuusvaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta.

2 Organisaation johdon keskeiset tietoturvavelvoitteet

Tiedot ja tietoturvallisuus ovat nykypäivän tietokeskeisessä yhteiskunnassa ehdottomia edellytyksiä organisaation toiminnalle. Keskeisten liiketoimintaa ja päätöksiä tukevien tietojen tulee olla saatavilla tarvittaessa. Organisaation toiminta voi lamaantua täysin ilman keskeisiä toimintaympäristön tarvitsemia tietoja, tietojärjestelmiä ja yhteyksiä. Tietojen tulee olla oikeita ja luotettavia. Päätökset, jotka perustuvat virheelliseen tai oikeudettomasti muutettuun tietoon, voivat aiheuttaa vakavia vahinkoja organisaation toiminnalle ja imagolle sekä yhteiskunnan turvallisuudelle. Tietojen asianmukaisesta salassapidosta on huolehdittava tiedon suojaustason edellyttämällä tavalla.

Asianmukaisella tietojen suojauksella turvataan organisaation toimintaympäristöä, yhteiskuntaa sekä asiakkaiden ja yhteistyökumppaneiden tietoja. Tietojen luvaton päätyminen sivullisille voi täyttää rikoksen tunnusmerkistön. Se voi myös vaarantaa toimintaympäristön turvallisuuden ja palveluiden jatkuvuuden tai rikkoa yksilöiden perusoikeuksia, yksityisyyden suojaa ja turvallisuutta. Organisaation tulee omaan toimintaan liittyvien tietojen salassapidon lisäksi huolehtia sidosryhmiensä ja erityisesti asiakkaidensa tiedoista. Muun muassa henkilötietoihin ja yritysten liike- ja ammattisalaisuuksiin liittyy salassapitovelvoite.

Johdon tulee kiinnittää erityistä huomioita organisaation kokonaisvaltaiseen tietoriskien hallintaan, joka kattaa sekä oman toiminnan että kaikki keskeiset sidosryhmät; asiakkaat, sopimuskumppanit ja toimeksiannosta toimivat. Tietoriskit nousevat usein yhdeksi keskeisimmistä riskienhallinnan osa-alueista. Erityisen haasteen muodostaa kasvava palvelu- ja sopimustoimittajien verkosto, joka tekee organisaatiot riippuvaisiksi ulkoisista sidosryhmistä. Näin tietoriskit eivät ole enää täysin omassa hallinnassa. Verkostoituminen liittyy ICT-palvelutoimituksiin, mutta myös muihin kone-, laite- ja palvelutoimituksiin, esimerkiksi siivous-, huolto- ja vartiointipalveluihin.

Asetus tietoturvallisuudesta valtionhallinnossa - 2010/681, 4 §.

Valtionhallinnon viranomaisen on pidettävä huolta, että tietoturvallisuuden suunnittelu hyvän tiedonhallintatavan mukaisesti perustuu viranomaisen selvityksiin ja arvioihin sen hallussa olevista asiakirjoista sekä niihin tallennettujen tietojen merkityksestä ja että suunnittelussa otetaan huomioon suojattavien tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset.

Organisaatioiden johto on keskeisessä asemassa tietoturvallisuuden ylläpitämisessä ja kehittämisessä. Tietoturvatyölle tulee nimetä vastuuhenkilö, esim. tietoturvapäällikkö sekä osoittaa hänelle riittävät resurssit hoitaa ja toteuttaa organisaation tietoturvavelvoitteita organisaation toimintaympäristön ja ulkoisten vaatimusten edellyttämällä tavalla. Tietoturvallisuus tulee organisoida ja vastuuttaa erityisesti riskienhallintatoimessa, tietohallintotoimessa, sopimus- ja hankintatoimessa, sekä lainmukaisuuden valvonnassa. Ilman johdon tukea tietoturvatyö ei voi saavuttaa sille asetettuja tavoitteita lainsäädännön velvoitteiden osalta eikä tuottaa tavoiteltuja hyötyjä. Tietoturvallisuutta voidaan hallita hallintajärjestelmällä, jossa määritetään keskeiset tietoturvavastuut, riskienhallintamenettelyt sekä kehitys-, seuranta- ja raportointiprosessit. Hallintajärjestelmä voidaan toteuttaa osaksi organisaation vallitsevia toiminnan suunnittelu ja seurantamekanismeja, esimerkiksi laatuohjelmaa

Organisaation johdon keskeiset tietoturvavelvoitteet voidaan tiivistää seuraaviin kymmeneen kohtaan, joita on tarkemmin selvitetty seuraavissa kappaleissa. Liitteessä 1 on esitetty tiiviissä muodossa Johdon tietoturvavelvoitteiden muistilista.

1. Lainmukaisuuden varmistaminen
2. Riskienhallinnan- ja hallintajärjestelmän toteuttaminen
3. Tietoturvapolitiikkaan sitoutuminen
4. Tietoturvajohtaminen
5. Tietoturvavastuuhenkilön nimeäminen
6. Tietoturvallisuuden organisointi
7. Tietoturvallisuuden toteutumisen varmistaminen
8. Tietoturvallisuuden TTS-suunnitteluedellytysten luonti
9. Poikkeama- ja erityistilanteiden hallinta
10. Tietoturvaraportointivelvollisuuksista huolehtiminen.

Kts. Liite 1 - Johdon keskeiset tietoturvavelvoitteet – Muistilista

2.1 Lainmukaisuus (1)

Tietoturvallisuus on valtionhallinnossa voimakkaassa muutostilassa. Tämä johtuu yhteiskunnan keskeisten toimintojen ja tarjottavien palveluiden sähköistymisestä sekä kasvavasta tietoteknisestä riippuvuudesta. Samalla myös turvallisuusuhkat ovat painottumassa yhä enemmän tietoverkkoihin, organisaatioiden arkaluonteisiin tietoihin, ja tietojärjestelmiin, mutta myös avainhenkilöihin, kansalaisiin sekä asiakkaisiin. Valtionhallinnossa tähän uhkaan on pyritty vastaaman lainsäädännön keinoin velvoittamalla organisaatioita tietoturvallisuuden kehittämiseen.

Johdon tulee varmistaa, että organisaatiossa on tunnistettu sitä koskeva keskeinen tietoturvallisuuden lainsäädäntö ja organisaatio täyttää sille asetetut tietoturvavelvoitteet, erityisesti tietoturva-asetuksen sekä sen perusteella annetut tietoturvatasojen vaatimukset.

Valtioneuvoston periaatepäätös tietoturvallisuudesta - 7/2009, Luku 1 4. mom..

Jokaisen viranomaisen tulee huolehtia siitä, että riittävän hyvä tietoturvallisuus ja henkilötietojen suoja toteutuvat omassa organisaatiossa ja yhteistyössä sidosryhmiensä kanssa sekä hankittaessa palveluita organisaation ulkopuolelta. Kansalaisille ja yhteisöille tarjottavien hallinnon palveluiden ja muun julkisen vallan käytön tulee tapahtua niin, että voidaan turvata riittävällä tavalla käytössä olevien tietojen, tuotettujen palveluiden ja järjestelmien tietoturvallisuus.

Keskeinen organisaatioita velvoittava tietoturvallisuuden lainsäädäntö ja normisto on seuraava:

- **Laki viranomaisten toiminnan julkisuudesta - 21.5.1999/621**
  Laissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista samoin kuin viranomaisten velvollisuuksista tämän lain tarkoituksen toteuttamiseksi.
- **Asetus tietoturvallisuudesta valtionhallinnossa - 1.7.2010/681**
  Asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvavaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvavaatimuksista.

- **Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (VAHTI 7/2009)**
  Päätös valtionhallinnon tietoturvallisuuden kehittämisestä, sen periaatteista ja painopisteistä sekä keskeiset linjaukset jokaisen viranomaisen tietoturvatyölle.
- **Laki kansainvälisistä tietoturvallisuusvelvoitteista - 588/2004**
  Laissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvavelvoitteiden toteuttamiseksi. Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.
- **Henkilötietolaki - 523/1999**
  Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.
- **Valtioneuvoston periaatepäätös yhteiskunnan turvallisuusstrategiasta 26.10.2010**
  Periaatepäätöksellä osaltaan ylläpidetään valtiollista itsenäisyyttä, yhteiskunnan turvallisuutta sekä väestön elinmahdollisuuksista kaikissa turvallisuustilanteissa.

Lisäksi tietoturvallisuutta koskevia velvoitteita on monissa toimialakohtaisissa erityislaeissa sekä henkilötietojen- ja yksityisyyden suojaa käsittelevissä laeissa.

Kts. Liite 2 – Tietoturvallisuuden Perustason toteuttaminen.

2.2 Riskienarviointi ja hallintajärjestelmä (2)

Tietoturvatoimenpiteiden tulee perustua organisaation toiminnan riskien arviointiin. Johdon tulee huolehtia siitä, että organisaatiossa tehdään säännönmukaista tietoriskien arviointia, joka on integroitu osaksi organisaation muuta riskienhallintaa, toiminnan suunnittelua tai laatumallia.

Tietoriskit tulee arvioida suhteessa vallitsevaan lainsäädäntöön, toimintaympäristön vaatimuksiin ja kustannuksiin. Riskienhallinnan toteutus tulee kuvata organisaation tietoturvallisuuden hallintajärjestelmässä sekä Sisäisen valvonnan arviointi- ja vahvistuslausumassa (kts. kohta 2.7)

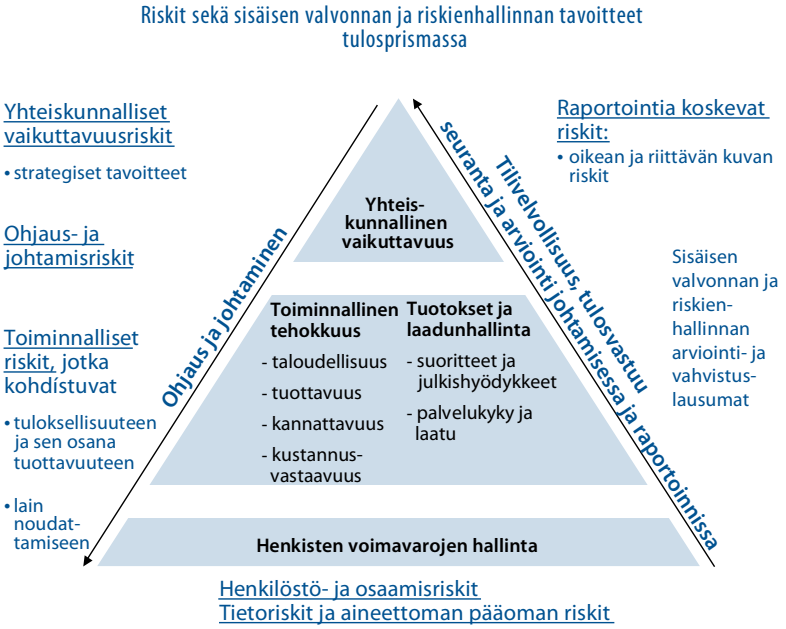
Tietoturvallisuus integroituu osaksi riskienhallintaa tietoriskien arvioinnin kautta. Tietoriskien arviointia tulee tehdä etupainotteisesti yhdessä muun riskienarvioinnin ja toiminnansuunnittelun kanssa. Tietoriskejä arvioidaan

organisaation perustehtävän ja sen saavuttamiseksi asetettujen strategioiden ja tavoitteiden kautta.

Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallintasuositus määrittää tietoriskien ja tietoturvallisuuden velvoitteista seuraavasti:

> Valtion virastojen ja laitosten toiminnan kannalta yhä tärkeämpiä voimavaroja ja toimintaedellytyksiä ovat henkiset voimavarat sekä informaatio ja tieto. Tämän mukaisesti henkilöstöön ja osaamiseen kohdistuvien riskien ja tiedon laatuun ja tietoturvallisuuteen (**tietoriskit**) hallinta on tärkeä osa riskienhallintaa.
>
> Valtion virastoissa, laitoksissa ja rahastoissa on hyvin harvoin tarkoituksenmukaista järjestää erillisiä riskienhallinnan prosesseja. **Kuitenkin esimerkiksi tietoturvallisuusriskien tunnistaminen ja hallinta vaativat yleensä erityistä asiantuntemusta ja omia menettelyitä.**
>
> Valtion viraston ja laitoksen tai rahaston riskienhallintapolitiikka voi useimmiten sisältyä toiminta- ja taloussuunnitelmiin, tulostavoiteasiakirjoihin sekä taloussääntöön ja **tietoturvallisuussuunnitelmiin** sekä muihin perusdokumentteihin eikä erillisen riskienhallintapolitiikkadokumentin laatiminen ole välttämätöntä.

KUVA 1. Organisaation tietoturvatavoitteet riskienhallinnan ja sisäisen valvonnan tulosprismassa



Tietoriskien arvioinnissa hyvä lähtökohta on lähteä liikkeelle organisaation tietoturvan perustason toteuttamisesta, joka organisaatioiden tulee täyttää viimeistään 30.9.2013.

Kts. Liite 3 - Tietoturvallisuutta ohjaava laatukehikko ja raportointikäytännöt.

2.3 Tietoturvallisuuden johtaminen (3, 4, 5)

Johdon tulee sitoutua tietoturvallisuuteen ja sen toteuttamiseen tietoturvapolitiikassa, jossa ilmaistaan johdon tahtotila tietoturvallisuuden toteuttamiseksi, kehittämisiksi sekä vastuut henkilöstö- ja esimiestasolla.

Johdon tulee osoittaa tietoturvallisuuteen riittävät resurssit ja huolehtia, että tietoturvallisuus toteutuu kaikilla tasoilla. Organisaatioon tulee nimetä tietoturvavastaava, jolla on tarvittava työaika käytettävissään tehtävän suorittamiseen.

Tietoturvallisuutta tulee käsitellä organisaation johtoryhmässä säännöllisesti, esim. neljännesvuosittain ja aina keskeisten tietoturvapoikkeamien tai -loukkausten tapahtuessa.

Tietoturvavastaavan tulee raportoida johdolle tietoturvallisuuden tilasta, kehityksestä ja tietoturvavelvoitteiden toteutumisesta. Johdon velvollisuus on varmistaa, että vastuuhenkilölle toimitetaan tarpeellinen tieto tietoturvallisuuden tilannekuvan muodostamiseksi.

Kts. Liite 4 – Esimerkki tietoturvapolitiikka (VAHTI 3/2007).

2.4 Tietoturvallisuuden organisointi (6, 7)

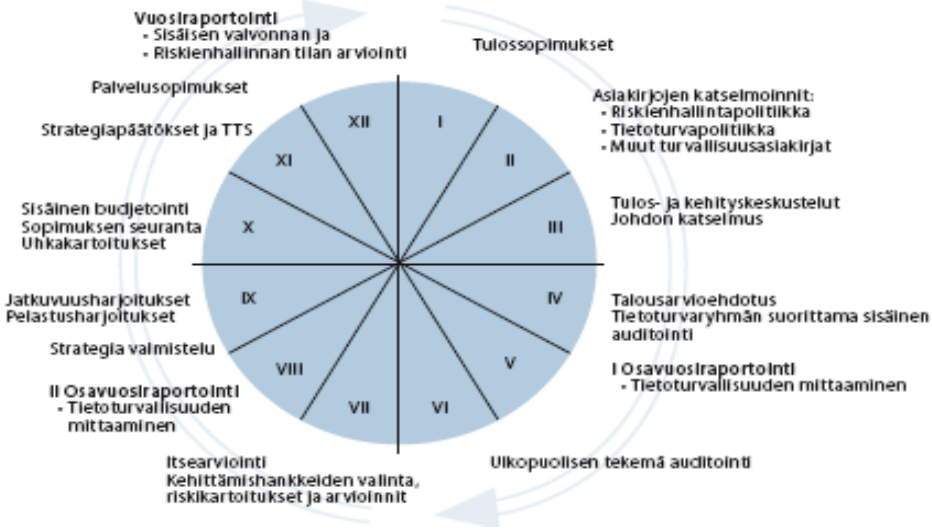
Organisaation vastuualueilla (osastoilla, yksiköissä ja toiminnoissa) tulee olla nimetyt tietoturvallisuuden vastuuhenkilöt, jotka edustavat tietoturvallisuuden yhteistyöryhmissä oman osa-alueensa tietoturvallisuutta. Johdon tulee varmistaa, että tietoturvallisuus huomioidaan ja sitä toteutetaan keskeisissä hallinnollisissa toiminnoissa, kuten tieto-, henkilöstö-, talous- ja materiaalihallinnossa sekä hankintatoimessa.

Johdon tulee huolehtia, että keskeisissä hankinnoissa (myös muissa kuin ICT-hankinnoissa), hankkeissa ja projekteissa sekä ICT-arkkitehtuurin kehittämisessä tietoturvallisuus huomioidaan tarvittavalla tasolla. Tietoturvapäällikölle tulee toimittaa tieto kaikista keskeisistä hankkeista ja kehittämistoimista sekä osallistaa tietoturvapäällikkö näihin liittyvään päätöksentekoon säännönmukaisesti.

2.5 Tietoturvallisuuden suunnittelu (8)

Tietoturvallisuudessa tulee tehdä vuosisuunnittelua samaan tapaan kuin muussakin toiminnoissa. Tietoturvapolitiikan ja sen perusteella luodun hallintajärjestelmän perusteella organisaation tulee toteuttaa tietoturvallisuuden vuosisuunnittelua, joka tulee integroida TTS-suunnitteluun. Organisaation johdon tulee huomioida TTS-suunnittelussaan tietoturvallisuuden tarvitsemat resurssit ja yksilöidä tietoturvallisuuden ylläpito- ja kehittämistoimet sekä budjetoida tästä aiheutuvat kustannukset.

KUVA 2. Esimerkki tietoturvallisuuden vuosikellosta



2.6 Poikkeama- ja erityistilanteiden hallinta (9)

Johdon tulee varmistaa, että organisaatiolla on edellytykset toimia poikkeama-, erityis-, ja kriisitilanteissa. Tietoturvallisuudessa tulee huomioida erityisesti ICT-varautumisen velvoitteet.

Poikkeama- ja erityistilanteiden hallinta on tärkeä osa organisaation toimintavarmuuden ja jatkuvuuden turvaamista. Organisaation johdon tulee varmistaa, että poikkeama- ja erityistilanteiden hallintakyky on olemassa, vastuut määritelty ja toimintatavat luotu. Keskeisessä roolissa on myös tiedottaminen ja viestintä sidosryhmille ja asiakkaille.

Erityistilanteilla tarkoitetaan häiriötilanteiden lisäksi myös organisaatiota koskettavia Yhteiskunnan Turvallisuusstrategiassa (YTS) kuvattuja tilanteita, joista suoriutumiseen tarvitaan koko organisaation sitoutumista ja kriisinhallintaa sekä tehtävien priorisointia. Tietoturvallisuudella on erityinen rooli toiminnan jatkuvuuden ja ICT-varautumisen suunnittelussa, suunnitelmien toteuttamisessa ja harjoittelussa. Johdon tulee varmistaa, että ICT-varautumiseen panostetaan riittävät resurssit ja se integroidaan osaksi koko organisaation valmiussuunnittelua.

2.7 Raportointi (10)

Organisaation johdon tulee raportoida tietoturvallisuuden tilasta ja kehittämisestä vuosittainen osana Sisäisen valvonnan ja riskienarvioinnin vahvistuslausumaa. Organisaatiolla tulee olla myös sisäinen tietoturvaraportointikäytäntö, joka toimii toiminnan kaikilla tasoilla ylhäältä-alas sekä alhaalta-ylös. Mikäli organisaatiolla on sisäinen laatujärjestelmä, on luontevaa integroida tietoturvallisuuden mittaaminen ja raportointi osaksi tätä järjestelmää.

Talousarvioasetuksen 65 §:n 7. kohdan mukaan on **viraston tai laitoksen, jolle ministeriö** on talousarvioasetuksen 11 §:ssä säädetyllä tavalla vahvistanut **tulostavoitteet**, laadittava kirjanpitoyksikön tilinpäätökseen kuuluva toimintakertomus, joka **sisältää sisäisen valvonnan arviointi- ja vahvistuslausuman**.

Kts. Liite 3 - Tietoturvallisuutta ohjaava laatukehikko ja raportointikäytännöt.

Liite 1. Johdon keskeiset tietoturvavelvoitteet – Muistilista

1. Lainmukaisuuden varmistaminen

Johdon tulee varmistaa, että organisaatiossa on tunnistettu sitä koskeva keskeinen tietoturvallisuuden lainsäädäntö ja organisaatio täyttää sille asetetut tietoturvavelvoitteet, erityisesti tietoturva-asetuksenmukaisuuden (1.7.2010/681 5 §) sekä sen perusteella annettujen tietoturvatasojen velvoitteet - Tietoturvallisuuden perustaso tulee täyttää 30.9.2013 mennessä.

2. Riskienhallinnan- ja hallintajärjestelmän toteuttaminen

Johdon tulee huolehtia, että organisaatiossa tehdään säännönmukaista tietoriskien arviointia, joka on integroitu osaksi organisaation muuta riskienhallintaa ja toiminnan suunnittelua. Tietoriskit tulee arvioida suhteessa vallitsevaan lainsäädäntöön, toimintaympäristön vaatimuksiin ja kustannuksiin. Toteutus tulee kuvata organisaation tietoturvallisuuden hallintajärjestelmässä sekä Sisäisen valvonnan arviointi- ja vahvistuslausumassa (kts. kohta 2.7)

3. Tietoturvapolitiikkaan sitoutuminen

Johdon tulee sitoutua organisaation tietoturvallisuuden toteuttamiseen ja ilmaista sitoutuminen tietoturvallisuuteen ja tietoriskienhallintaan organisaation tietoturvapolitiikassa ja tämän pohjalta laaditussa tietoturvaohjeistuksessa.

4. Tietoturvajohtaminen

Tietoturvallisuutta tulee käsitellä organisaation johtoryhmässä säännöllisesti, esim. neljännesvuosittain ja aina keskeisten poikkeama- tai tietoturvaloukkausten tapahtuessa.

5. Tietoturvavastuuhenkilön nimeäminen

Johdon tulee nimetä organisaatioon tietoturvavastaava, jonka tulee raportoida johdolle tietoturvallisuuden tilasta, kehityksestä ja tietoturvavelvoitteiden toteutumisesta. Johdon velvollisuus on varmistaa, että tietoturvallisuuden vastuuhenkilöllä on tarvittavat toimintaedellytykset ja vastuuhenkilölle toimitetaan tarpeellinen tieto tietoturvallisuuden tilannekuvan muodostamiseksi.

6. Tietoturvallisuuden organisointi

Johdon tulee varmistaa, että tietoturvallisuus on vastuutettu organisaation tietoturvallisuuden kehittämisen kannalta keskeisissä toiminnoissa ja kaikilla substanssitoimialoilla sekä tukitoiminnoissa.

7. Tietoturvallisuuden toteutumisen varmistaminen

Johdon tulee huolehtia, että keskeisissä hankinnoissa (myös muissa kuin ICT-hankinnoissa), hankkeissa ja projekteissa sekä ICT-arkkitehtuurin kehittämisessä tietoturvallisuus huomioidaan tarvittavalla tasolla. Tietoturvavastaavalle tulee toimittaa tieto kaikista keskeisistä hankkeista ja kehittämistoimista sekä osallistaa tietoturvavastaava näihin liittyvään päätöksentekoon säännönmukaisesti.

8. Tietoturvallisuuden TTS-suunnitteluedellytysten luonti

Organisaation johdon tulee huomioida TTS-suunnittelussaan tietoturvallisuuden tarvitsemat resurssit ja yksilöidä tietoturvallisuuden ylläpito- ja kehittämistoimet sekä budjetoida niistä aiheutuvat kustannukset.

9. Poikkeama- ja erityistilanteiden hallinta

Johdon tulee varmistaa, että organisaatiolla on edellytykset toimia poikkeama-, erityis-, ja kriisitilanteissa. Tietoturvatyössä tulee huomioida erityisesti ICT-varautumisen velvoitteet.

10. Tietoturvaraportointivelvollisuuksista huolehtiminen

Organisaation johdon tulee raportoida tietoturvallisuudesta osana vuosittaista Sisäisen valvonnan ja riskienhallinnan vahvistuslausumaa.

Liite 2. Tietoturvallisuuden perustason toteuttaminen

Valtionhallinnon toimijoiden tulee täyttää tietotruvallisuusasetuksessa asetetut tasot asetuksessa annetussa aikataulussa; tietoturvallisuuden perustaso 30.9.2013 mennessä.

Tietoturvallisuuden perustason täyttäminen edellyttää asetuksen mukaisesti alla kuvattuja toimenpiteitä. Tietoturvatasojen tarkemmat toteuttamisohjeet ja vaatimukset löytyvät julkaisusta Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010).

Asetus tietoturvallisuudesta valtionhallinnossa - 1.7.2010/681 5 §:

Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:

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

Valtionhallinnon viranomaisen velvollisuudesta huolehtia tietojen suojaamisesta annettaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten säädetään viranomaisten toiminnan julkisuudesta annetun lain 26 §:n 2 momentissa. Henkilörekisteriin talletettujen henkilötietojen antamisesta säädetään lisäksi henkilötietolain 32 §:n 2 momentissa.

Liite 3. Tietoturvallisuutta ohjaava laatukehikko ja raportointikäytännöt

Onnistunut ja oikein mitoitettu tietoturvatyö perustuu toimivaan tietoturvajohtamiseen, jonka vaatimuksia on esitetty tietoturvatasojen vaatimuksissa (kts. VAHTI 2/2010). Tietoturvallisuuden johtamista voidaan kehittää ja mitata laadunhallinnan kautta samaan tapaan, kuin muutakin johtamista. Johtamisen laatujärjestelmän arviointikriteeristöä voidaan käyttää tietoturvatasovaatimusten nykytilan ja kehittämisen tukena, jonka avulla voidaan pureutua syvemmälle organisaation tietoturvajohtamisen mekanismeihin ja arvioida sen vaikuttavuutta ja tarvittavia kehittämistoimia.

Yhteinen arviointimalli (CAF – Common Assessment Framework) on julkisen sektorin organisaatioille tarkoitettu laadunarviointityökalu. Se sisältää vaikutteita Euroopan laatupalkintomallista (EFQM). Yhdeksän arviointialuetta sisältävä malli kattaa kaikki organisaation toiminnan arvioinnin kannalta keskeisimmät osa-alueet. Ensimmäiset viisi arviointialuetta tarkastelevat niitä organisaation toimintatapoja, joilla pyritään saavuttamaan asetetut tavoitteet ja tavoitellut tulokset. Jälkimmäisellä neljällä alueella arvioidaan näistä toimintatavoista seuraavia tuloksia eri näkökulmista. Organisaation EFQM-malliin voidaan liittää myös tietoturvallisuuden arviointikriteerejä tai käyttää mallia puhtaasti tietoturvajohtamisen arviointiin.

Kokonaisvaltaisessa tietoturvajohtamisessa ja sitä toteuttavassa hallintajärjestelmässä tarvitaan toiminnan suunnittelua, kattava dokumentaatio, raportointikäytännöt (kts. alla Taulukko 2) sekä toimivat mittarit. Yksinomaan toimintaperiaatteiden ja suunnitelmien olemassaolo ei tuota laatua, vaan sen edellytyksenä ovat käytännössä toteutetut johdon määrittämät toiminnot ja niillä saavuttavat tulokset.

Seuraavassa taulukossa on kuvattu esimerkin omaisesti CAF-laarviointimenetelmän tietoturvallisuuden pääkriteerejä jaoteltuna arviointialueittain sekä arvioinnin mahdollisia kohteena olevia asiakirjoja.

TAULUKKO 1. Esimerkki EFQM-mallin tietoturvallisuusjohtamisen kriteereistä.

Arviointialue	Tietoturvallisuuden arviointikriteerit	Vastaava tietoturvatasoalue	Esimerkkejä arvioitavista kohteista ja asiakirjoista
Johtajuus	Tietoturvallisuuden organisointi, vastuut ja raportointikäytännöt sekä johdon tuki	• Strateginen ohjaus • Resursointi ja organisointi • Yhteistyön koordinointi • Raportointi ja viestintä sidosryhmille • Johtaminen erityistilanteissa • Raportointi johdolle	Tietoturvapolitiikka ja vastuut, tietoturvavastaava, johdon ja vastuuhenkilöiden yhteistyö, tietoturvaryhmä, tietoturvapoikkeamien käsittelyn organisointi ja johdolle raportointi. **Työjärjestys, organisaatiokaavio, johtoryhmien pöytäkirjat, suunnitellut ja tehdyt kehittämistoimet.**
Strategiat ja toiminnan suunnittelu	Tietoturvallisuus strategioissa ja tulostavoitesopimuksissa	• Toimintaympäristön vaikutus • Tavoitteiden määrittely • Toiminnan kehittäminen riskien arvioinnilla • Toimintaverkoston hallinta • Erityistilanteiden hallinta.	Toimintaympäristön tietoturvallisuuden erityisvaatimukset ja tavoitteet. Ydintoimintojen ja -prosessien suojattavat kohteet, luokittelu ja tietoturvataso. Tietoriskien arviointiprosessi. Toimintaverkostot, sopimuskumppanit ja alihankkijat. Jatkuvuussuunnittelu. **Tulostavoitesopimukset, strategia-asiakirjat, turvallisuuspolitiikka, tietoturvapolitiikka.**
Henkilöstöjohtaminen	Tietoturvaosaaminen ja sen sisällyttäminen toimintatapoihin	• Osaamisen ja tietoisuuden kehittäminen ja sanktiot • Henkilöresurssien ja tehtävien hallinta • Erityistilanteissa toiminen.	Henkilöstön, avainryhmien ja tietoturvahenkilöstön osaaminen tietoturvakoulutus ja perehdyttäminen sekä ohjeista tiedottaminen. Sääntöjen noudattamisen seuranta ja poikkeamista ilmoittaminen sekä niihin puuttuminen. Tietoturvallisuuden avainroolien tunnistaminen ja varahenkilöt. **Virkaehtosopimus, työsopimus, perehdytysmateriaali, vaitiolositoumus, koulutussuunnitelma.**
Kumppanuudet ja resurssit	Tietoturvallisuuden hallinta yhteistyösuhteissa, teknologiassa, tiedon ja tietämyksen hallinnassa sekä fyysisen toimintaympäristön hallinnassa. Ulkoistaminen ja turvallisuuden hallinta. Palvelujen hankinnan. tietoturvallisuus.	• Sopimusten hallinta • Toiminnan varmistaminen erityistilanteissa.	Kumppanuus- ja hankintatoiminen vastuut ja organisointi, sopimuskäytännöt sekä tietoturvavelvoitteet. **Sopimukset ja sopimuskäytännöt, hankintaohjesääntö.**

Arviointialue	Tietoturvallisuuden arviointikriteerit	Vastaava tietoturvatasoalue	Esimerkkejä arvioitavista kohteista ja asiakirjoista
Prosessit ja muutosjohtaminen	Tietoturvallisuuden hallinta prosessien kehittämisen, suunnittelun ja järjestelmällisen hallinnan osana omassa ja yhteistyökumppaneihin liittyvissä prosesseissa sekä tietoturvallisuuden prosessien jatkuva kehittäminen	• Tietoaineistojen hallinta.	Tietoturvallisuuden ja sen osa-alueiden organisointi ja hallinta: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteisto-turvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. **Tietoturvallisuuden hallintajärjestelmä, sidosryhmäyhteistyömalli.**
Asiakas- ja kansalaistulokset	Tietoturvallisuuden mittarit ja tulosten seuranta asiakkaiden, kansalaisten ja suorituskyvyn näkökulmista	• Toiminnan arviointi ja todentaminen.	Organisaation saavuttamat tulokset tietoturvallisuuden näkökulmasta suhteessa asiakkaiden ja kansalaisten odotuksiin. Esim. asiakkaille ja kansalaisille tarjottavien palveluiden tietoturvallisuus (saatavuus, eheys ja luottamuksellisuus). **Kaupalliset palvelu- ja turvallisuussopimukset ja näissä määritellyt tietoturvakontrollit, mittarit sekä tulokset.**
Henkilöstötulokset	Motivaatio, tyytyväisyys ja suorituskyky, tietoturvatyön osaaminen, sitoutuminen	• Toiminnan arviointi ja todentaminen.	Organisaation saavuttamat tulokset pyrkiessään vastaamaan henkilöstön tarpeisiin ja odotuksiin tietoturvallisuuden huolehtimisesta ja toteuttamisesta. **Työhyvinvoinnin arviointitulokset, tietoturvakoulutukset ja tentit, tietoturvallisuuteen sitouttamistoimet, henkilöstön väärinkäytökset ja tämän perusteella tehdyt toimet.**
Yhteiskunnalliset tulokset	Vastuu yhteiskunnan toimintavarmuudesta ja turvallisuusstrategiavelvoitteista. Turvallisen toimintaympäristön ja tietoturvallisuuden kehittämistulokset. Turvallisuutta vaarantavien tapahtumien havainnointi ja näiden perusteella tehdyt korjaavat toimenpiteet..	• Toiminnan arviointi ja todentaminen.	Millaisia vaikutuksia organisaation toiminnalla on ollut yhteiskunnallisiin tietoturva-asioihin mm. kansalliset ja kansainväliset tietoturvavelvoitteet, tietoturvallisuusasetuksen mukaisuus, Yhteiskunnan turvallisuusstrategia. **Tietoturvatasojen auditointiraportti, muut tietoturvallisuuden arviointiraportit. Ulkoiset auditointiraportit, esim. tietoturvatasoauditointitulokset.**

Arviointialue	Tietoturvallisuuden arviointikriteerit	Vastaava tietoturvatasoalue	Esimerkkejä arvioitavista kohteista ja asiakirjoista
Keskeiset suorituskykytulokset	Tietoturvallisuuden vaikuttavuuden mittaaminen poikkeamatilanteiden ja kehitystoimien toteutumisen kautta.	• Toiminnan arviointi ja todentaminen	Suorituskykytulokset organisaation pitkän ja lyhyen aikavälin välttämättömiksi sekä mitattaviksi ja arvioitaviksi tietoturvatavoitteiksi, mm. tietoturvallisuusasetuksen velvoitteiden täyttäminen, kansainvälisten tietoturvavelvoitteiden täyttäminen sekä toimintavarmuuden kannalta keskeisten häiriö- ja poikkematilanteiden hallinta. **Tietoturvataso- sekä muut sisäiset ja ulkoiset auditointiraportit. Tietoturvallisuuden kehityssuunnitelmat, poikkeamatilanneraportit, valmius- ja jatkuvuussuunnitelmat.**

Tietoturvallisuuden seurannan ja raportoinnin tulee olla jatkuvaa ja aktiivista.

Tietoturvaraportointi on yksi keskeinen tietoturvallisuuden johtamisen mekanismi tarvittavien kehitystoimien tunnistamiseksi sekä tilannekuvan muodostamiseksi. Johdon tulee olla tietoinen organisaation tietoturvallisuuden tilasta ja vaikuttavuudesta. Johdon tulee pystyä myös reagoimaan välittömiä toimenpiteitä vaativiin poikkeamatilanteisiin. Tilannekuvan muodostava valvonta ja raportointi suunnitellaan siten, että resurssit suunnataan tietoturvallisuuden kannalta merkityksellisimpiin suojattaviin kohteisiin, kuten tärkeimpiin prosesseihin, tietojärjestelmiin, tietovarastoihin sekä tietoturvaohjeiden noudattamiseen. Seuraava taulukko kuvaa esimerkinomaisesti organisaation keskeisiä raportointikäytäntöjä.

TAULUKKO 2. Organisaation raportointikäytännöt.

	Raportointiaika	Aihe
1	Välitön raportointi johdolle	Hetkellinen, toimintaa vaarantava tapahtuma: Ihmisiin, omaisuuteen, tietoon tai toimintavarmuuteen kohdistuva, jonka korjaaminen vaatii välittömiä toimenpiteitä: erityistilanne, vakava uhka, vakava vahinko.
2	Säännöllinen raportti organisaation johdolle tietoturvapolitiikan mukaisesti	Tietoturvallisuuden tilanneraportti (mahdollisesti osana muuta raportointia) sekä päivitetty tilannekuva.
3	Vuosiraportointi johdolle tietoturvapolitiikan mukaisesti.	Johdon yhteenveto tietoturvallisuuden poikkeamatilanteista, tietoturvallisuuden tilasta ja keskeisistä kehittämistoimista ja kehittämistarpeista..
4	Ajantasainen tilannekuva tietoturvavastaavalle.	Yhteenveto tapahtuneista keskeisistä poikkeamista ja korjaavista toimenpiteistä.
5	Jatkuva raportointi keskeisten toimintojen ja näitä tukevien järjestelmien vastuuhenkilöille.	Järjestelmän toimintaa ja tietoturvallisuutta uhkaavat tai vaarantavat tilanteet sekä tehdyt toimenpiteet.

Liite 4. Esimerkki Tietoturvapolitiikka (VAHTI 3/2007)

Esimerkki organisaation tietoturvapolitiikasta, jota tulee käyttää organisaation koon ja toimintaympäristön mukaan soveltaen.

1. Johdanto

Johdon sitoutuminen, ”lausuma” tietoturvallisuustyöhön sitoutumisesta sekä määrittelyt organisaation tietoturvallisuusvastuista sekä toteuttamistavoista.

2. Tietoturvapolitiikan tavoite

2.1. Tietoturvallisuuden käsite ja merkitys
2.2. Määritelmät

Tietoturvatyön sisällön määrittely, tietoturvallisuuden suojattavien kohteiden tunnistaminen sekä työn tavoitteet suojattavien kohteiden turvaamiseksi.

3. Tietoturvatoimintaa ohjaavat tekijät

Organisaation tietoturvallisuutta velvoittavat ja ohjaavat kansalliset ja kansainväliset yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut tietoturvallisuutta ohjaavat velvoitteet, määräykset ja ohjeet.

4. Tietoriskien hallinta

Kuvaus organisaation tietoriskien hallintaprosessista. Uhkien tunnistus ja vaikutusanalyysin muodostaminen sekä tarvittavista toimenpiteistä päättäminen riskien hallitsemiseksi.

5. Tietoturvallisuuden merkitys organisaatiolle

5.1. Toiminnan kannalta elintärkeät palvelutehtävät
5.2. Tietoturvaperiaatteet
5.3. Tietoturvallisuuden toteutumista tukevia käytäntöjä

Yleiskuvaus organisaation toimintaympäristön tietokriittisyydestä sekä keskeisistä palveluista, prosesseista ja toiminnoista sekä näiden jatkuvuuden ja toimintavarmuuden hallintamekanismeista. Tietoturvallisuuden keskeiset periaatteet ja velvoitteet sekä näiden toteuttamista ohjaavat toimintatavat.

6. Turvatoimien priorisointi

Mahdollinen suojattavien kohteiden priorisointi ja perustelut.

7. Tietoturvallisuuden hallintajärjestelmä

Kuvaus tietoturvallisuuden hallintajärjestelmästä ja sen toteuttamiseksi sovituista prosesseista sekä vuosikellosta.

8. Tietoturvavastuut

8.1. Organisaation tietoturvavastuut
8.2. Organisaation yhteistyökumppaneiden vastuut

Kuvaus tietoturvavastuista eri tasoilla organisaation sisällä sekä sidosryhmien, asiakkaiden ja yhteistyökumppaneiden suuntaan. Myös tietoturvavastuut organisaatiota kohtaan keskeisten sidosryhmien ja yhteistyökumppaneiden osalta.

9. Tietoturvakoulutus ja -ohjeet

Kuvas tietoturvaohjeistuksen, koulutuksen ja perehdyttämisen periaatteista ja käytännöistä.

10. Tietoturvallisuudesta tiedottaminen

Tietoturvallisuuden tiedottamis- ja viestintäkäytännöt ajankohtaisasioista, ohjeista sekä poikkeamatilanteista.

11. Tietoturvallisuuden toteutumisen valvonta

Tietoturvallisuuden valvonta ja raportointivelvoitteet arkityössä sekä havaituissa poikkeamatilanteissa.

12. Toiminta poikkeustilanteissa ja -oloissa

Kuvaus yhteiskunnan turvallisuustilanteiden ja poikkeamatilanteiden johtamisvastuista ja menettelytavoista.

Liite 5. Voimassa olevat VAHTI-julkaisut

- Johdon tietoturvaopas, VAHTI 2/2011
- VAHTIn toimintakertomus vuodelta 2010, VAHTI 1/2011
- Sosiaalisen median tietoturvaohje, VAHTI 4/2010
- Sisäverkko-ohje, VAHTI 3/2010
- 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
- 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

2/2011
VAHTI
Joulukuu 2011

ISSN 1455-7606 (nid.)
ISBN 978-952-251-279-6 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-280-2 (pdf)