



318/31/2011

17.10.2011

VM/1509/00.00.00/2011 Lausuntopyyntö johtajan tietoturvaoppaasta

LAUSUNTO JOHTAJAN TIETOTURVAOPPAASTA

Ajatuksena johdon tietoturvaopas johdolle suunnattuna käsikirjamaisena ohjeena on kannatettava. Ohje tulisi pystyä tiivistämään luonnoksen luvussa 2 esitetyllä tavalla johdon huoneentauluksi tai toimenpideluetteloksi.

Oppaan rakennetta tulisikin tiivistää. VAHTI-ohjeen tasoisessa julkaisussa jokaisen sanan ja lauseen tulisi olla tarkkaan harkittu ja sisältää jonkin merkityksen. Nyt näin ei ole. Lisäksi luonnoksessa käytetyissä käsitteissä on horjuvuutta. Johdolle suunnatun VAHTI-ohjeen sanamuodot olisi hyvä olla sellaisia, että niistä ei synny mielikuvaa, että ohjeen kautta pyrittäisiin vaikuttamaan organisaatioiden sisäiseen työnjakoon. Lausunnon liitteeseen on koottu esimerkkejä muutosehdotuksineen luvun 1 ja luvun 2.1 tarkistettavista teksteistä.

Luonnoksen luvussa 2 on lueteltu kymmenen tietoturvavelvoitetta, ja ilmeisesti seuraavissa alaluvuissa näitä velvoitteita on ollut tarkoitus käsitellä tarkemmin. Alaluvuissa käytetään kuitenkin eri otsikoita tai jäsentelyä kuin aikaisemmin olevassa luettelossa (esim. lainmukaisuuden varmistaminen – lainmukaisuus) tai niissä ei tuoda juurikaan mitään uutta aikaisemmin esitettyyn luetteloon nähden (esim. alaluvut 2.3-2.5).

Luonnoksen liitteet tulisi kytkeä oppaan tekstiin ja mainita selvästi niiden tarkoitus oppaan osana. Epäselväksi jää esimerkiksi, tuleeko johdon toimeenpanna liitteessä 2 esitetty laatukehikko ja raportointi, vai miksi kyseinen liite on oppaassa mukana.

Lausunnossa ei oteta kantaa kirjoitusvirheisiin, jotka – samoin kuin valtionhallinnossa käytettävät käsitteetkin - olisi ollut suhteellisen vaivatonta korjata jo lähetettyyn luonnokseen. VAHTI-ohjeen luonnokselta olisi odottanut, että tietoturvallisuudesta annetun valtioneuvoston asetuksen voimaantulopäivämäärä olisi ollut oikein.

Ohjeluonnos on palautettava takaisin valmisteluun. Ehdotetaan, että uudelleen valmistelussa johdanto on enintään sivun mittainen, luvussa kaksi selvitetään johdon velvoitteet ja että liitteenä on yksisivuinen kymmenen kohdan huoneentaulu ja tekstiin sidottuna ehkä yksi tai kaksi muuta liitettä esimerkkeinä.

Pääjohtaja

Tuomas Pöysti

Tietojohtaja

Jaakko Hamunen

LIITE

Tarkistettavaa tekstiä luvuista 1 ja 2.1

VALTIONTALOUDEN TARKASTUSVIRASTO

► Postiosoite: PL 1119, 00101 Helsinki ► Käyntiosoite: Antinkatu 1, 00100 HELSINKI
► Puhelin: (09) 4321 ► Faksi: (09) 432 5820

TIETOTURVAOPPAAN TARKISTETTAVAA TEKSTIÄ LUVUISTA 1 ja 2.1

1 Johdanto tietoturvallisuuden johtamiseen

”Tietoturvallisuudella suojataan lainmukaisuusperiaatteen mukaisesti organisaation...” Ehdotetaan poistettavaksi ”lainmukaisuusperiaatteen mukaisesti”

”Tietoturvallisuus tulee organisoida ja tietoturvallisuutta toteuttaa siten, että se tukee parhaalla mahdollisella ja kustannustehokkaalla tavalla organisaation lainmukaisuuden toteuttamista, hyvää hallintotapaa sekä perustehtävä- ja strategiatavoitteiden saavuttamista.” Ehdotetaan, että tämä muutetaan esimerkiksi muotoon ”Tietoturvallisuus tulee organisoida ja tietoturvallisuutta toteuttaa siten, että se tukee parhaalla mahdollisella ja kustannustehokkaalla tavalla organisaation lakisäätteisten tehtävien toteuttamista” tai muuhun ymmärrettävään muotoon.

”Tietoturvallisuuden tulee olla osa organisaation kokonaisvaltaista riskienhallintaa, jossa tietoturvallisuus muodostaa perustan toiminnan jatkuvuussuunnittelulle ja toimintavarmuudelle.” Tietoturvariskien hallinta voidaan mieltää osaksi organisaation riskienhallintaa. Jatkuvuussuunnittelun perustan muodostanee organisaation lakisäätteisten tehtävien turvaaminen häiriötilanteissa ja poikkeusoloissa.

”Keskeisten liiketoimintaa ja päätöksiä tukevien tietojen tulee olla saatavilla tarvittaessa.” Ehdotetaan, että valtionhallinnon organisaatioiden käyttöön tarkoitettussa oppaassa käytetään muuta käsitettä kuin liiketoiminta.

”asiakkaiden liike- ja ammattisalaisuuksia” Valtionhallinnon organisaatioiden asiakkaista suurin osa lienee muita kuin sellaisia, joilla on liike- ja ammattisalaisuuksia.

”Tietojen luvaton päätyminen sivullisille on lainrikkomus” ehdotetaan muutettavaksi muotoon ”...voi olla..”

”Muun muassa henkilötietoihin ja yritysten liike- ja ammattisalaisuuksiin liittyy salassapitovelvoite.” ehdotetaan muutettavaksi muotoon ”...voi liittyä...”

”Yhteiskunnan tietoturvariskien hallitsemiseksi ja tietoturvallisuuden kehittämiseksi valtionhallinnossa on 1.7.2010 astunut voimaan Asetus tietoturvallisuudesta valtionhallinnossa.” Mikäli tällä tarkoitetaan valtioneuvoston asetusta tietoturvallisuudesta valtionhallinnossa, niin se on kyseisen asetuksen 22 §:n mukaan astunut voimaan 1 päivänä lokakuuta 2010. Ehdotetaan myös tarkistettavaksi onko asetus annettu luonnoksessa mainitussa tarkoituksessa, sillä aina-kaan asetuksen 1 § asetuksen soveltamisalasta ei mainitse tietoturvariskien hallitsemisesta ja tietoturvallisuuden kehittämisestä.

2 Organisaation johdon keskeiset tietoturvavelvoitteet

Tietoturvapäällikkö. Ehdotetaan, että tekstissä puhutaan tietoturvallisuuden vastuuhenkilöstä kuten luvussa 1 ja luvun 2 kohdan 5 otsikossa.

Tietoturvallisuuden toteutumisen varmistaminen. Mikäli kyseissä kohdassa käsitellään vain hankintoja, hankkeita ja projekteja, ehdotetaan muutettavaksi kohdan otsikko vastaavasti. Jos taas on tarkoitus käsitellä tietoturvallisuuden toteutumisen varmistamista, niin silloin kohdassa tulisi käsitellä monia muitakin asioita.

”Tietoturvapäällikölle tulee toimittaa tieto kaikista keskeisistä hankkeista ja kehittämistoimista sekä osallistaa tietoturvapäällikkö näihin liittyvään päätöksentekoon säännönmukaisesti.”

VALTIONTALOUDEN TARKASTUSVIRASTO

Ehdotetaan muutettavaksi muotoon ”Tietoturvavastaava voidaan nimetä mukaan kehityshankkeisiin osallistumaan hankkeiden riskikartoituksiin, -arviointeihin ja riskien hallintatoimenpiteiden suunnitteluun ja toteutukseen”

”Tietoturvallisuuden TTS-suunnitteluedellytysten luonti” ehdotetaan muutettavaksi muotoon ”Tietoturvallisuuden suunnittelu” ja ”TTS-suunnittelussaan” ehdotetaan muutettavaksi muotoon ”toiminnan ja talouden suunnittelussa”. Tämä sanamuoto kattaisi paremmin sekä tulossuunnittelukauden ja toiminta- ja taloussuunnittelukauden suunnittelun.

2.1 Lainmukaisuus (1)

Mikäli otsikko on lainmukaisuus, niin olisi johdonmukaista että otsikon alla käsiteltäisiin lainsäädännön asettamia velvoitteita. Nyt otsikon alle on kerätty muutakin kuin vain lainsäädäntöä.

”Tietoturvallisuus on valtionhallinnossa voimakkaassa kehityksessä. Tämä johtuu yhteiskunnan keskeisten toimintojen ja tarjottavien palveluiden sähköistymisestä sekä kasvavasta tietoteknisestä riippuvuudesta. Samalla myös turvallisuusuhkat ovat painottumassa yhä enemmän tietoverkkoihin ja organisaatioiden arkaluonteisiin tietoihin, tietojärjestelmiin ja myös avainhenkilöihin, kansalaisiin sekä asiakkaisiin. Valtionhallinnossa tähän uhkaan on pyritty vastaamaan lainsäädännön keinoin panostamalla organisaatioiden tietoturvallisuuden kehittämiseen.” Epäselväksi jää, miten edellä oleva lainaus liittyy lainmukaisuuteen, ovatko tietoturvallisuuden voimakkaan kehityksen syyt todella tekstissä mainitut ja mitkä ovat ne lainsäädännölliset keinot, joilla on panostettu organisaatioiden tietoturvallisuuden kehittämiseen.