

Asia: VM136:09/2013

## **Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta**

Yleistä ohjeeseen liittyen

**Yleiset kommentit ja havainnot ohjeeseen**

-

### **1. Johdanto**

**Lausuntomme:**

-

### **2. Tietoturvapoikkeaman hallintaprosessi**

**Lausuntomme:**

-

### **3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen**

**Lausuntomme:**

Sivu 11. Taulukko kolme. Voisiko taulukkoon kirjoittaa, että henkilötietoihin kohdistunut väärinkäytöstä tulee ilmoittaa tietosuojavaltuutetulle.

Sivu 12. Olisiko mahdollista laittaa tähän Kyberturvallisuuskeskuksen yhteystietoja esimerkiksi sähköposti-osoitetta tai www-sivua?

Sivu 12. Eikö ”poliisi” kohtaan olisi hyvä laittaa tieto siitä, että rikosilmoituksen voi tehdä sähköisesti? Olisiko lisäksi mahdollista laittaa linkki tai sposti-osoite yhteydenottoja varten?

Sivulla 13. kuitenkin mainitaan poikkeuksena muista VTV:n www-sivu.

Sivu 13. 3.3.7. ”Kansallinen turvallisuusviranomainen” eikö voisi mainita, mikä taho on ko. viranomainen? Mainittu kuitenkin taulukossa 3.

Sivu 13. 3.3.8. EU:n tietosuoja-asetuksen valvova viranomainen

Tarkoitetaan varmaan tietosuojavaltuutettua – ei tietoturvaltuutettua.

Voisi laittaa myös linkin TSV:n sivuille tai laittaa posti-osoitteen minne ilmoituksen voi tehdä.

## 4. Tietoturvapojikkeaman havaitseminen ja analysointi

**Lausuntomme:**

-

## 5. Tietoturvapojikkeamaan reagointi

**Lausuntomme:**

Sivu 23.

5.1.4. Esimerkkejä erilaisista poikkeamatilanteista

Olisiko nämä hyvä laittaa erilliseen liitteeseen? Eli sivut 23- 26.

Sivu 28. 3.3.8. EU:n tietosuoja-asetuksen valvova viranomainen ja 5.3.3. Viestintä henkilötietoihin kohdistuvissa poikkeamissa tulisi linkittyä toisiinsa ja olla yhdenmukaisia. Yhtäkkiä ne näyttävät samalta asialta mutta eivät ole saman sisältöisiä – viittaus toiseen ainakin puuttuu.

## 6. Toipuminen tietoturvapojikkeamatilanteista

**Lausuntomme:**

-

## Liite 1. Sanasto

**Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?**

Sivu 31 – 33. LIITE 1. Sanasto

Olisiko tähän mahdollista saada myös termin englanninkielinen / ruotsinkielinen versio rinnalle?

## Liitteet 2-5

### Lausuntomme:

Sivu 34. Varmaan huomasitte? Onko yhdenmukainen?

"CERT-toiminnassa vakiintunut Traffic Light Protocol -käytäntö on saanut ensimmäisen standardiksi kutsuttavan määritelmän. Päivitimme omaa TLP-ohjettamme vastaavaan uutta standardimääritelmää.

Tässä asiaa taustoittava Tietoturva nyt! -artikkeli:

<https://www.viestintavirasto.fi/2016/10/ttn201610061413>

Ja tässä uusi ohjeemme:

<https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuosittelujenja-selvitystenasiakirjat/yhteistyoryhmientiedonvaihtokaytantoja0032016j.html> "

## Liitteet 6-9

### Lausuntomme:

-

### Vaatimus-Excel ja vaatimukset

**Palaute, kommentit ja kehittämisideat koskien vaatimuksia**

-

**Ehdotetut perustason vaatimukset ovat**

-

**Muuta palautetta tai toiveita ohjeluonnokseen liittyen**

**Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTille?**

-

**Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:**

Hyvin

Aitta Matti  
Oikeusministeriö