



DIGI- JA  
VÄESTÖTIETO-  
VIRASTO

# Digiturmajahti

VAHTI hyvät käytännöt -tukimateriaali

6.2.2022



## Sisällysluettelo

1	Johdanto .....	2
2	Taustaa .....	2
3	Tavoite .....	3
4	Digiturmajahti-malli .....	3
4.1	Esimerkki Digiturmajahti-mallin ohjeista ja säännöistä .....	4
4.2	Viestintä .....	5



# Digiturmajahti

## 1 Johdanto

Tämä VAHTI hyvät käytännöt -tukimateriaali on laadittu julkisen hallinnon organisaatioille turvallisen työskentelyn ja toiminnan edistämiseksi. Tukimateriaali pohjautuu julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) asiantuntijaryhmien kokoamiin riskienhallinnan, toiminnan jatkuvuuden ja valmiuden, tietoturvallisuuden, tietosuojan ja kyberturvallisuuden hyviin käytäntöihin. Toimimalla hyvien käytäntöjen mukaisesti edistämme digitaalisen turvallisuuden toteutumista.

Toivomme, että annat meille palautetta tästä Digiturmajahti-mallista. Otamme parannus- ja korjausehdotuksia vastaan ja julkaisemme mallista päivitetyn version saatamme riittävästi uusia kehittämissuhteita.

[Linkki palautelomakkeeseen](#)

Jokainen organisaatio ja asiantuntija vastaa siitä, että tätä tukimateriaalia käytettäessä sen sisältö sovitetaan organisaation toimialaan ja sitä koskevaan lainsäädäntöön.

VAHTI hyvät käytännöt -tukimateriaalit on ensisijaisesti suunnattu julkisen hallinnon organisaatioille, mutta mikä tahansa organisaatio voi ottaa niitä vapaasti käyttöönsä. Mikäli kehittäte tai muuten parannatte tukimateriaaleja, toivomme, että annatte niistä meille palautetta sisällön jatkokehittämiseksi.

## 2 Taustaa

Digitaalisen turvallisuuden kehittämisestä vastaavat ensisijaisesti organisaation riskienhallinnan, jatkuvuudenhallinnan ja varautumisen, kyberturvallisuuden, tietoturvan ja tietosuojan vastuuhenkilöt. Lisäksi organisaation johdon tehtävänä on huolehtia organisaation digitaalisen toimintaympäristön turvallisuuden ja luottamuksen mahdollistavista linjauksista ja resursseista.

Digitaalisen maailman turvallisuudesta huolehtiminen on kuitenkin meidän kaikkien vastuulla niin työpaikalla, työmatkalla, etänä työskenneltäessä kuin vapaa-ajallakin. Useissa tutkimuksissa onkin nostettu esille se, kuinka juuri käyttäjät aiheuttavat erilaisia tietoturvaan tai tietosuojaan liittyviä poikkeamia, jotka saattavat vaarantaa organisaatioiden toiminnan esimerkiksi henkilötietojen tai salassa pidettävien tietojen osalta. Poikkeamia voi syntyä myös teknisten järjestelmien virheellisten asetusten tai ohjelmistoissa piilevien haavoittuvuuksien vuoksi. Niitä saattavat aiheuttaa ulkoiset, ennalta arvaamattomat seikat. Poikkeaman taustalla voi olla tietoinen ohjeiden vastainen toiminta tai jopa tarkoituksellinen vahingonteko. Erilaisiin poikkeamiin on kuitenkin mahdollista varautua: keskeisessä roolissa ovat tietoisuuden lisääminen, ennakointi ja organisaation toiminnan jatkuva kehittäminen.



### 3 Tavoite

Tässä hyvät käytännöt -dokumentissa kuvattavalla Digiturmajahti-mallilla kannustamme organisaatioita käynnistämään digitaalista turvallisuutta edistävän kampanjan. Mallin tarkoituksena on kannustaa henkilöstöä tekemään havaintoja ja ilmoituksia sellaisesta organisaation toiminnasta tai henkilöstön työskentely- ja toimintatavoista, jotka voivat vaarantaa organisaation toiminnan tai sen käsittelemiä tietoja sekä aiheuttaa taloudellisia vahinkoja, mainehaittoja tai muita organisaation toimintaa haittaavia seurauksia.

Mallin perusteella käynnistettävällä organisaatiokohtaisella kampanjalla kannustetaan henkilöstöä ottamaan mahdollisimman matalalla kynnyksellä yhteyttä organisaation turvallisuudesta vastaaviin henkilöihin silloin, kun työntekijät havaitsevat turvallisuuspoikkeamia tai haluavat antaa kehittämissuhteita.

Joissakin organisaatioissa on ollut käytössä Bug Bounty -haavoittuvuuspalkkio-ohjelmia. Digiturmajahti poikkeaa kyseisistä ohjelmista siten, että Bug Bounty on tarkoitettu tietojärjestelmien ja -palveluiden, sovellusten sekä verkkojen teknisten haavoittuvuuksien tunnistamiseen ja niiden raportoimiseen tarkkaan sovitulla mallilla. Digiturmajahti on tarkoitettu puolestaan enemmän muiden kuin teknisten digitaaliseen turvallisuuteen liittyvien poikkeamien havaitsemiseen ja niiden raportoimiseen.

Koska teknisiä, valkohattu- tai hyväshakkereille tarkoitettuja Bug Bounty -ohjelmia saatetaan tehdä testiympäristön sijaan toiminnassa olevassa tuotantoympäristössä, ohjelman toteuttaminen, ohjeiden laatiminen ja ohjelmaan osallistuvien sitoutuminen ohjeiden noudattamiseen on erittäin tärkeää. Kannustamme organisaatioita toteuttamaan myös teknisiä Bug Bounty -ohjelmia, koska ne edistävät kriittisten palveluiden ja sovellusten turvallisuutta. Niissä jaettavat palkintosummat voivat olla merkittävästi tässä dokumentissa kuvattua mallia korkeampia, jopa kymmeniätuhansia euroja.

### 4 Digiturmajahti-malli

Digiturmajahti voidaan käynnistää halutuksi määräajaksi tai siitä voidaan tehdä toistaiseksi voimassa oleva toimintamalli. Suositeltavaa on ensin pilotoida mallia määräaikaista, jotta se tulee henkilöstölle tutuksi. Pilotin jälkeen siihen voidaan tarvittaessa tehdä korjauksia pilotoinnin perusteella, jos organisaatio haluaa luoda siitä pysyvän toimintamallin.

Jokainen mallin käyttöön ottava organisaatio voi myös harkita, haluaako se kutsua omia sidosryhmiään mukaan kehittämään digitaalista turvallisuutta. Tällöin organisaatio voi esimerkiksi tiedottaa toimiloissaan vierailevia henkilöitä Digiturmajahdistista ja pyytää heitä ilmoittamaan mahdollisista havainnoistaan.

Alla olevaa esimerkkimallia ei saa julkaista sellaisenaan, vaan jokaisen organisaation tulee sovittaa se omaan toimintaansa ja saada toimintamallille organisaation johdon hyväksyntä. Keskeiset muokkausta vaativat kohdat on korostettu **keltaisella**.



Toivomme, että Digiturmajahti innostaa tekemään tällaisia ilmoituksia myös jatkossa, vaikka niistä ei välttämättä myönnettäisikään erityisiä tunnustuksia.

## 4.1 Esimerkki Digiturmajahti-mallin ohjeista ja säännöistä

### Yleistä

Digiturmajahti on uusi tapa kehittää organisaation digitaalisen turvallisuuden osa-alueita kuten riskienhallintaa, toiminnan jatkuvuutta, tietoturvaa, tietosuoja ja kyberturvallisuutta, sekä tätä kautta edistää digitaalisen turvallisuuden toteutumista. Digiturmajahti ei edellytä erityistaitoja tai -osaamista, vaan se on tarkoitettu meille kaikille!

Digiturmajahti mahdollistaa sen, että kuka tahansa voi ilmoittaa organisaatiossa havaitsemistaan turvallisuuspuutteista ja -kehittämiskohteista, mahdollisista uhkista ja riskeistä sekä muista seikoista organisaation turvallisuudesta vastaaville henkilöille.

Otamme vastaan myös havaittujen puutteiden ja kehittämiskohteiden ohella avointa palautetta, toteuttamiskelpoisia ideoita sekä kysymyksiä, joihin lupaamme vastata.

Digiturmajahdin aikana annamme tunnustuksen kaikista sellaisista havainnoista ja ilmoituksista, jotka johtavat turvallisuutta edistäviin tai korjaaviin toimenpiteisiin.

### Palkitseminen

Jokainen Digiturmajahti-ilmoitus käsitellään. Julkaisemme kerran kuukaudessa sellaiset Digiturmajahti-ilmoitukset, jotka ovat johtaneet korjaaviin toimenpiteisiin. Nämä ilmoitukset julkaistaan anonyymisti | nimimerkillä | nimellä.

Myönnämme näistä turvallisuutta edistävästä ilmoituksista tunnustuksen | palkkion | palkattoman vapaan | lahjakortin | muu tapa seuraavasti.

#### 1. taso

- Ilmoituksen avulla pystymme hieman parantamaan toimintamme turvallisuutta.

o palkkio – lahjakortti, arvo 20 € | tai muu organisaation valitsema tapa

#### 2. taso

- Ilmoituksen avulla pystymme parantamaan jonkin verran toimintamme turvallisuutta.

o palkkio – lahjakortti, arvo 40 € | tai muu organisaation valitsema tapa

#### 3. taso

- Ilmoituksen avulla pystymme parantamaan merkittävästi toimintamme turvallisuutta.





- o palkkio – lahjakortti, arvo 100 € | tai muu organisaation valitsema tapa

#### Erityistunnustus

- Ilmoitettu havainto on erityisen merkittävä. Sen avulla voimme välttää meihin kohdistuvan merkittävän riskin tai kehittää organisaatiomme turvallisuutta huomattavasti.
  - o erikseen ilmoituksen tehneen henkilön kanssa sovittava verollinen palkkio | muu palkitsemistapa

**Huom.** Organisaation tulee itse selvittää ja kuvata tavat, joilla se voi palkita henkilöstöään ottaen huomioon mahdolliset veroseuraamukset.

#### Kuinka ilmoituksen voi tehdä?

Voit tehdä ilmoituksen seuraavilla tavoilla:

1. lähettämällä sähköpostia osoitteeseen [digiturmajahti@<organisaatio>](mailto:digiturmajahti@<organisaatio>)
  - o Kuvaa ehdotuksesi, mahdollinen uhka, tunnistamasi riski tai havaitsemasi turvallisuuspoikkeama mahdollisimman tarkasti.
  - o Haluatko, että ilmoituksesi julkaistaan nimelläsi, antamallasi nimimerkillä vai anonyymisti?
2. täyttämällä Digiturmajahti-ilmoituslomakkeen osoitteessa <https://intranet>
3. jokin muu organisaation määrittämä ilmoitustapa.

Lisätietoa kampanjasta antaa **Nimi** ja **sähköpostiosoite**.

Kehitetään #digiturvaa yhdessä!

## 4.2 Viestintä

Organisaation kannattaa viestiä kampanjasta säännöllisesti sekä sisäisesti että halutessaan ulkoisesti. Suosittelemme, että organisaation johto ja esihenkilöt vastaavat sisäisestä viestinnästä. Kampanjan edistämiseksi siitä kannattaa kertoa organisaation yhteisissä tilaisuuksissa sekä muistuttaa asiasta myös esihenkilöiden ja työntekijöiden välisissä säännöllisissä keskusteluissa.

Organisaatio voi lisäksi halutessaan ohjeistaa, miten henkilöstö voi tuoda omaa osallistumistaan esille sosiaalisen median kanavissa. Suositeltavaa on käyttää tällöin tunnistetta #digiturmajahti. Organisaation kannattaa miettiä huolella tämä ohjeistus, jotta kukaan ei kuvittele, että varsinaiset ilmoitukset tulee tehdä sosiaalisen median kanaviin.

Mikäli organisaatio pilotoi Digiturmajahti-mallia tai ottaa sen pysyvästi käyttöön, olemme kiinnostuneita kuulemaan käyttökokemuksista ja saamaan siitä palautetta.



6.2.2022

Erityisesti toivomme tietoa sellaisista kehittämiskohteista, jotka ovat sovellettavissa laaja-alaisesti myös muihin organisaatioihin. Käsittelemme saadun palautteen anonyymisti, ellei organisaatio erikseen anna lupaa nimensä julkaisemiseen. Halutessaan organisaatio voi myös ilmoittautua referenssiksi muille toimintamallista kiinnostuneille organisaatioille.

Palautteet ja yhteydenotot Digiturmajahti-mallista voi toimittaa sähköpostitse osoitteeseen [digiturva@dvv.fi](mailto:digiturva@dvv.fi).

### Lisätiedot

Kimmo Rousku, VAHTI-pääsihteeri, [kimmo.rousku@dvv.fi](mailto:kimmo.rousku@dvv.fi)  
Juha Kirves, erityisasiantuntija, [juha.kirves@dvv.fi](mailto:juha.kirves@dvv.fi)