Digiturvan kokonaiskuva -kysely

Digiturvan kokonaiskuvapalvelu on DVV:n kehittämä ja ylläpitämä palvelu, joka kerää tietoa julkisen hallinnon organisaatioiden digitaalisen turvallisuuden tilanteesta.

Lisää tietoa palvelusta ja siihen liittymisestä löytyy osoitteesta https://dvv.fi/digiturvajulkaisut (ks. Ohjeet-osio).

Organisaation tilannetta kartoittava kysely sisältää seuraavat hallinnollisen digitaalisen turvallisuuden tilaa koskevat väittämät.

Kunkin väittämän vastausvaihtoehdot ovat Kyllä – Osittain – Ei – Ei koske meitä
Joissain väittämissä on lisätietoja, jotka auttavat vastaamisessa.

Väittämän nro	**1**
Osa-alue	**Johtaminen**
Kuvaus	Organisaation tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.
Lisätiedot	

Väittämän nro	**2**
Osa-alue	**Johtaminen**
Kuvaus	Organisaatio on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.
Lisätiedot	– kattaa kaikki digitaalisen turvallisuuden osa-alueet

---

Väittämän nro	**3**
Osa-alue	**Johtaminen**
Kuvaus	Organisaatio on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.
Lisätiedot	– lainsäädännölliset ja sopimukselliset velvoitteet

---

Väittämän nro	**4**
Osa-alue	**Johtaminen**
Kuvaus	Organisaatiossa on riittävästi osaavaa henkilöstöä digiturvallisuuden eri osa-alueilla.
Lisätiedot	– digiturvallisuudesta vastaavia henkilöitä on riittävästi ja heillä on riittävä osaaminen

---

Väittämän nro	**5**
Osa-alue	**Johtaminen**
Kuvaus	Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon sekä kehittämiseen.
Lisätiedot	

Väittämän nro	**6**
Osa-alue	**Johtaminen**
Kuvaus	Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.

Lisätiedot	– Organisaation johto on viestinyt ja osoittanut riittävässä määrin tukevansa digitaalisen turvallisuuden toteuttamista ja kehittämistä

Väittämän nro	**7**
Osa-alue	**Johtaminen**
Kuvaus	Organisaation digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia.
Lisätiedot	– esim. ISO-standardin mukainen tai muu yleinen hallintamalli

---

Väittämän nro	**8**
Osa-alue	**Johtaminen**
Kuvaus	Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta.
Lisätiedot	– mm. – hyväksyttävän käytön periaatteet ja tarkempi ohjeistus – tietoaineistojen käsittelyohjeet sisältäen esimerkiksi ohjeet henkilötietojen ja salassa pidettävien tietojen käsittelystä eri palveluissa – toimitilojen tietoturvallisuutta koskevat ohjeet – tietosuojaperiaatteet – Onko ohjeistus ja prosessit jalkautettu ja miten se pystytään osoittamaan?

Väittämän nro	**9**
Osa-alue	**Johtaminen**
Kuvaus	Henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.
Lisätiedot	– onko digitaalinen turvallisuus huomioitu henkilöstön perehdytyksessä? – onko henkilöstön säännöllistä koulutusta digitaalisesta turvallisuudesta? – onko otettu huomioon eri rooleihin ja työtehtäviin liittyvät erityistarpeet? – onko osaamisen ylläpitäminen säännönmukaista toimintaa? – koulutussuunnitelma – koulutus- ja perehdytysmateriaalit

---

Väittämän nro	**10**
Osa-alue	**Johtaminen**
Kuvaus	Organisaatiolla on olemassa prosessi väärinkäytöksiin reagoimiseksi.
Lisätiedot	– kuvattu prosessi, vastuut ja seuraamukset

Väittämän nro	**11**
Osa-alue	**Johtaminen**
Kuvaus	Digitaaliseen turvallisuuteen liittyvät mittarit on määritelty.
Lisätiedot	– mittarit on määritelty (tavoitteiden pohjalta) ja niihin liittyvää dataa kerätään jatkuvasti

---

Väittämän nro	**12**
Osa-alue	**Johtaminen**
Kuvaus	Digitaalisen turvallisuuden tilaa seurataan jatkuvasti.

Lisätiedot	– kattaa sekä hallinnollisen että teknisen seurannan

---

Väittämän nro	**13**
Osa-alue	**Johtaminen**
Kuvaus	Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti organisaation johdolle.
Lisätiedot	– vähintään kerran vuodessa

Väittämän nro	**14**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatiolla on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.
Lisätiedot	– riskienhallintapolitiikka tai vastaava

Väittämän nro	**15**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.
Lisätiedot	– prosessi ja vastuut kuvattuna, ja näyttöä prosessin toimivuudesta

---

Väittämän nro	**16**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatiossa viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko organisaation laajuisesti.
Lisätiedot	– digiturvasta vastaavien ja viestinnän yhteistyönä

Väittämän nro	**17**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatiossa raportoidaan riskitilanteesta johdolle säännöllisesti.
Lisätiedot	– vähintään kerran vuodessa

Väittämän nro	**18**
Osa-alue	**Riskienhallinta**
Kuvaus	Kriittisistä, organisaation toimintaa uhkaavista riskeistä raportoidaan johdolle välittömästi.
Lisätiedot	– prosessi kuvattuna ja näyttöä sen toimivuudesta

Väittämän nro	**19**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatio seuraa riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.
Lisätiedot	– kuvattu menettely ja näyttöä sen toimivuudesta

Väittämän nro	**20**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatiossa arvioidaan jäännösriskejä riskienhallintatoimenpiteiden toteuttamisen jälkeen ja jäännösriskit käsitellään asianmukaisella tasolla.
Lisätiedot	– johto tai ko. toiminnon/riskin omistaja tekee tarvittavat päätökset

Väittämän nro	**21**
Osa-alue	**Riskienhallinta**
Kuvaus	Organisaatiossa kehitetään riskienhallintaprosessia saatujen riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.
Lisätiedot	

Väittämän nro	**22**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaation tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.
Lisätiedot	– kuvattu esim. valmiussuunnitelmassa

Väittämän nro	**23**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatiolla on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.
Lisätiedot	– poikkeamanhallintaprosessi ja vastuut kuvattuina

Väittämän nro	**24**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatio on kuvannut jatkuvuuden hallinnan periaatteet, tavoitteet, organisoinnin ja vastuut.
Lisätiedot	– jatkuvuudenhallinnan periaatteet tai vastaava

Väittämän nro	**25**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatio on tunnistanut ja dokumentoinut suojattavat kohteet.
Lisätiedot	– mm. henkilöstö, tilat, tietojärjestelmät, laitteet jne. – Organisaation käytössä olevat järjestelmät, palvelut ja laitteet (sisäiset ja ulkoiset) sekä niiden turvallisuuteen vaikuttavat asiat. – Organisaation tietovarannot, niiden kuvaukset, tiedonkäsittelyprosessit, vastuut, riskit ja suojaustoimet.

Väittämän nro	**26**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaation on tunnistanut sen toiminnan kannalta kriittiset toiminnot, palvelut, tiedot, tietovarannot ja tietojärjestelmät.

Lisätiedot	– kriittisyyden määrittelyyn on olemassa kuvattu menetelmä

Väittämän nro	**27**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatio on määritellyt kuinka pitkiä toimintakatkoksia kriittiset toiminnot sietävät organisaation toiminnan häiriintymättä.
Lisätiedot	– Organisaatio tuntee lainsäädännön vaatimukset liittyen sen järjestelmien, rekistereiden ja palveluiden saatavuuteen. – Organisaatio tuntee oman toiminnan ja sidosryhmien vaatimukset.

Väittämän nro	**28**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Toiminnan jatkuvuuden edellyttämät palvelutasovaatimukset ovat osa hankintavaatimuksia ja sopimuksia.
Lisätiedot	– mm. SLA, RPO, RTO

Väittämän nro	**29**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti.
Lisätiedot	– mm. SLA, RPO, RTO

Väittämän nro	**30**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin.
Lisätiedot	– prosessi kuvattuna ja näyttöä sen toimivuudesta

Väittämän nro	**31**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Kriittisille tietojärjestelmille on laadittu toipumissuunnitelmat.
Lisätiedot	– Sisältää mm. häiriötilanteen johtamiseen liittyvät menettelyt ja vaihtoehtoiset toimintatavat

---

Väittämän nro	**32**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatiolla on häiriö- ja kriisitilanteiden viestintäsuunnitelma.
Lisätiedot	– Viestinnän kohderyhmät, välineet, vastuut ja pääviestit – Myös suunnitelma vaihtoehtoisten viestintätapojen käytöstä, kun puhelin ja viestintäverkot eivät ole käytettävissä organisaatiossa tai sen sidosryhmillä ja asiakkailla

---

Väittämän nro	**33**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**

Kuvaus	Suunnitelmien sisältö on koulutettu häiriötilanteiden hallintaan osallistuville henkilöille.
Lisätiedot	

Väittämän nro	**34**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatiossa on luotu yhteydet ja verkostot tarvittavien sidosryhmien väliseen viestintään poikkeamatilanteissa.
Lisätiedot	– yhteystahot ja menettelyt kuvattu

Väittämän nro	**35**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatiolla on olemassa menettely sen toimintaa kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille.
Lisätiedot	– mm. Poliisi, Tietosuojavaltuutetun toimisto, Kyberturvallisuuskeskus

---

Väittämän nro	**36**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.
Lisätiedot	– vähintään kerran vuodessa (valitun osa-alueen osalta) – dokumentaatio harjoitusten toteutumisesta ja havainnoista

---

Väittämän nro	**37**
Osa-alue	**Toiminnan jatkuvuus ja varautuminen**
Kuvaus	Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella
Lisätiedot	– näyttö päivityksestä

Väittämän nro	**38**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaatiolla on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.
Lisätiedot	– mm. tavoitteet, periaatteet, organisointi, vastuut

---

Väittämän nro	**39**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön.
Lisätiedot	– kuvattu menettely ja näyttöä sen toimivuudesta

Väittämän nro	**40**
Osa-alue	**Tietoturvallisuus**

Kuvaus	Organisaatiolla on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.
Lisätiedot	– dokumentoitu prosessi

Väittämän nro	**41**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Käyttövaltuuksien ajantasaisuus varmistetaan säännöllisesti.
Lisätiedot	– menettelyt kuvattu, tarkistus vähintään vuosittain

---

Väittämän nro	**42**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaatio on määrittänyt fyysisesti suojatut turvallisuusalueet asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi.
Lisätiedot	– dokumentaatio ja ohjeistus

Väittämän nro	**43**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaation tietojärjestelmät ja laitteet ovat kattavasti järjestelmänhallinnan piirissä.
Lisätiedot	– mm. prosessit automaattisiin päivityksiin

Väittämän nro	**44**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaatiolla on käytössä monivaiheinen tunnistus etäkäytössä.
Lisätiedot	– MFA, Multi-Factor Authentication tai vastaava

Väittämän nro	**45**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Toimitilojen ulkopuolella työskenneltäessä yhteydet organisaation ICT-palveluihin sallitaan vain VPN-yhteydellä.
Lisätiedot	

Väittämän nro	**46**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaatiolla on olemassa tarvittavat tekniset ratkaisut ja menettelyt haittaohjelmien tunnistamiseen ja estämiseen.
Lisätiedot	– toteutus yhdyskäytävä- ja työasematasolla sekä tarvittava ohjeistus henkilöstölle

---

Väittämän nro	**47**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Organisaation tiedoista ja järjestelmistä otetaan säännöllisesti varmuuskopiot.
Lisätiedot	– kuvattu menettely ja näyttöä sen toimivuudesta

Väittämän nro	**48**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Varmuuskopioiden palautusta testataan säännöllisesti
Lisätiedot	– ainakin kriittisten palveluiden osalta

Väittämän nro	**49**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään riittävät lokitiedot.
Lisätiedot	– lainsäädännön ja toiminnan vaatimukset on selvitetty ja toteutettu lokitus niiden mukaisesti – Huomioitava Tiedonhallintalaki 17 § ja siitä annettu suositus

Väittämän nro	**50**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Käytössä olevien tietojärjestelmien teknisiin haavoittuvuuksiin liittyviä tiedotteita seurataan ja niihin reagoidaan.
Lisätiedot	– olemassa oleva menettely ja näyttöä sen toimivuudesta

Väittämän nro	**51**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.
Lisätiedot	– sisältää hallinnolliset ja tekniset auditoinnit – järjestelmiin vähintään käyttöönottovaiheessa sekä kriittisyyden mukaan säännöllisesti

Väittämän nro	**52**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.
Lisätiedot	– ovat hankinnoissa ns. pakollisia vaatimuksia

Väittämän nro	**53**
Osa-alue	**Tietoturvallisuus**
Kuvaus	Tietoturva- ja tietosuojavaatimukset otetaan huomioon myös järjestelmien ja palveluiden kehittämisessä sekä ylläpidossa.
Lisätiedot	– kuvattu menettely ja näyttöä sen toimivuudesta

Väittämän nro	**54**
Osa-alue	**Tietosuoja**
Kuvaus	Organisaatiolla on tiedossa, millaisia henkilötietoja se käsittelee (TsA 4 art. 1 kohta)
Lisätiedot	– nimi, osoite, sähköpostiosoite, puhelinnumero jne. – hetu (TSL 29 §) – erityiset henkilötietoryhmät (TsA 9 art. TSL 6 §) – rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot (TsA 10 art., TSL 7 §)

– Turvakiellon alaiset henkilötiedot
– Henkilöstön (TtsL), asiakkaiden, vierailijoiden, sidosryhmien henkilötiedot

---

Väittämän nro	**55**
Osa-alue	**Tietosuoja**
Kuvaus	Henkilötietojen käsittelyn oikeusperusteet on tunnistettu (TsA 6, 9 ja 10 art. TsL 6 ja 29 §, TtsL 2, 3, 5 ja 6 luku)
Lisätiedot	– suostumus – sopimus – lakisääteinen velvoite (edellyttää säännöksen yksilöintiä) – elintärkeä etu – yleinen etu ja julkinen valta (edellyttää säännösten yksilöintiä, yleisenedun yksilöintiä ja julkisen vallan säädösperustaa) – oikeutettu etu – Käsittelyn erityisedellytykset on huomioitu mm. seuraavissa tapauksissa – erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyperusteet – rikostuomioihin ja rikkomuksiin liittyvä käsittely – henkilötunnuksen käsittely – henkilötietojen käsittely työsuhteen yhteydessä

Väittämän nro	**56**
Osa-alue	**Tietosuoja**
Kuvaus	Organisaatio on tunnistanut, milloin se toimii rekisterinpitäjänä ja milloin se toimii käsittelijänä (TsA 4 art. 7-8 kohta)
Lisätiedot	– On olemassa prosessi tai ohjeistus rekisterinpitäjän ja käsittelijän tunnistamiseksi

---

Väittämän nro	**57**
Osa-alue	**Tietosuoja**
Kuvaus	Sopimukset henkilötietojen käsittelystä on tehty ja sopimusten hallinta on kunnossa (TsA 28 art)
Lisätiedot	– Onko tietosuoja sisäänrakennettu hankintaprosessiin? – Onko henkilötietojen käsittelyn vaatimukset ja ehdot huomioitu henkilötietojen käsittelijöiden kanssa tehdyissä sopimuksissa? – Onko sopimusten hallintamalli laadittu? – Onko siirrot 3. maihin otettu huomioon?

Väittämän nro	**58**
Osa-alue	**Tietosuoja**
Kuvaus	Yhteisrekisterinpitäjyystilanteet tunnistetaan ja yhteisrekisterinpitäjyyttä koskevista vastuista on sovittu? (TsA 26 art., huom. myös EDPB:n ohje)
Lisätiedot	– Tunnistetaanko tilanteet, joissa on kyse yhteisrekisterinpitäjyydestä? – Onko yhteisrekisterinpitäjien vastuunjaosta sovittu tiedon keräämisestä sen hävittämiseen/arkistointiin? – Ovatko roolit ja vastuut selkeitä ja läpinäkyviä rekisteröidyille? – ohje tai prosessi, joka auttaa tunnistamaan yhteisrekisterinpitäjyyden ja siihen liittyvät roolit – sopimukset – viestintä rooleista ja vastuunjaosta rekisteröidylle

Väittämän nro	**59**
Osa-alue	**Tietosuoja**
Kuvaus	Henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu (TihL 4.2. §, TsA 37 art.)
Lisätiedot	– rekisterien omistajat / vastuuhenkilöt – johdon vastuut – esimiehet – henkilöstö – valvonta – tietosuojavastaava – muut roolit (tiedonhallinta, tietosuoja, tietoturva, riskienhallinta, tilaturvallisuus)

Väittämän nro	**60**
Osa-alue	**Tietosuoja**
Kuvaus	Tietosuojavastaavan asema ja rooli on määritelty (TsA 37 – 39 art.)
Lisätiedot	– tarve tietosuojavastaavan nimeämiseen on selvitetty – Tietosuojavastaavan sijaisjärjestelyt kunnossa, yhteydenotot poissaolon aikana – tietosuojavastaavan tehtävät ja asema ovat laissa säädetyn mukaiset – päätös tietosuojavastaavan nimeämisestä – esim. asema määritelty hallintosäännössä, työjärjestyksessä tms. – tehtävänkuvaus

Väittämän nro	**61**
Osa-alue	**Tietosuoja**
Kuvaus	Seloste käsittelytoimista on laadittu (TsA 30 art.)
Lisätiedot	– Sisältääkö vaaditut tiedot? – Toteutuvatko tietosuojaperiaatteet organisaatiosi toiminnassa? (TsA 5 art.) – lainmukaisuus, kohtuullisuus, läpinäkyvyys – käyttötarkoitussidonnaisuus – tietojen minimointi – täsmällisyys – säilytyksen rajoittaminen – eheys ja luottamuksellisuus

Väittämän nro	**62**
Osa-alue	**Tietosuoja**
Kuvaus	Organisaatiolla on tiedossa missä tietojärjestelmissä henkilötietoja käsitellään
Lisätiedot	– tietojärjestelmäsalkku/rekisteri – tietovirtakuvaukset – aputiedostot/listaukset

Väittämän nro	**63**
Osa-alue	**Tietosuoja**
Kuvaus	Rakenteeton tieto on tunnistettu ja sen hallinta on kuvattu
Lisätiedot	– Satunnaisten, ei-jäsenneltyjen sähköisten tietojen tunnistaminen ja hallinta – Tietoa käsitellään sellaisissa ympäristöissä, joissa tiedon elinkaarta ei pystytä metatietojen avulla hallitsemaan.

– esim. sähköpostiviestit, verkkolevyllä olevat tiedostot, Teams-tiimien tiedostot, Skype-/Teams-keskusteluhistoria

---

Väittämän nro	**64**
Osa-alue	**Tietosuoja**
Kuvaus	Informointikäytännöt on määritelty ja niitä noudatetaan (TsA 12-14 art. Laki digitaalisten palveluiden tarjoamisesta (306/2019)
Lisätiedot	– Otetaan huomioon informoinnin kohderyhmä sekä käsittelyn laajuus ja luonne valittaessa informointikäytäntöä. – Pystyttävä osoittamaan, että rekisteröity on saanut informaation – onko informaatio ymmärrettävää ja saavutettavaa

---

Väittämän nro	**65**
Osa-alue	**Tietosuoja**
Kuvaus	Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi (TsA 35 (1) art.)
Lisätiedot	– onko tunnistettu, milloin tulee suorittaa vaikutustenarviointi tai ennakkokuuleminen? – onko vakioitu prosessi kriteerien tunnistamiseksi olemassa?

Väittämän nro	**66**
Osa-alue	**Tietosuoja**
Kuvaus	Organisaatiolla on olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi (TsA 33-34 art.)
Lisätiedot	– vakioitu prosessi olemassa loukkausten käsittelemiseksi ja dokumentoimiseksi? – ilmoituskanavan määrittäminen ja vastuuhenkilöt ilmoitusten käsittelyyn – viranomaisilmoitusten tekeminen, päätöksentekovastuu ilmoituksista – rekisteröidyille ilmoittaminen – Miten varmistetaan henkilöstön kyvykkyys tunnistaa tietoturvaloukkauksia? – kuvaus prosessista

---

Väittämän nro	**67**
Osa-alue	**Tietosuoja**
Kuvaus	Jos henkilötietoja siirretään kolmansiin maihin, organisaatio on selvittänyt siirron edellytykset? (TsA 5 luku)
Lisätiedot	– Onko ymmärretty, mitä tarkoitetaan siirrolla kolmansiin maihin (esim. pääsy tietoihin kolmannesta maasta)? – Onko tunnistettu ne tilanteet, joissa tapahtuu siirtoja kolmansiin maihin? – Onko vaatimusmäärittelyssä huomioitu ne tilanteet, joissa siirrot kolmansiin maihin ei ole mahdollista? – Onko huomioitu siirrot kolmansiin maihin koko alihankintaketjussa? – Sopimuksen kolmansiin maihin siirtoja koskevat ehdot

---

Väittämän nro	**68**
Osa-alue	**Tietosuoja**
Kuvaus	Organisaatiossa tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi (TSA 5 art.)
Lisätiedot	– Mieti, miten kykenet arvioimaan toiminnan, kulttuuri ja asenteen muuttumista organisaatiossasi.

– esim. johdolle ja henkilöstölle kohdennetut kyselytutkimukset
– palvelulupaus tietosuojan huomioonottamisesta organisaation toiminnassa
– tietosuojapolitiikka
– vuosikello
– osaamisen mittaaminen

Väittämän nro	**69**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatio on huomioinut digitaalisen turvallisuuden osana kokonaisarkkitehtuuria.
Lisätiedot	– ainakin tietoturvallisuus

Väittämän nro	**70**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria.
Lisätiedot	– nimetty vastuuhenkilö ja aikaa tehtäviin

Väittämän nro	**71**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatio on tunnistanut oman roolinsa YTS:n mukaisissa tehtävissä sekä globaalissa näkökulmassa
Lisätiedot	– Miten riippuvainen yhteiskunta on organisaation tuottamista palveluista? – Riski hybridi- / informaatiovaikuttamiseen sekä siihen varautuminen

---

Väittämän nro	**72**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan.
Lisätiedot	– palvelut, joista muiden organisaatioiden operatiivinen toiminta on riippuvainen

---

Väittämän nro	**73**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatiossa on kattavasti tunnistettu kriittisten palveluiden riippuvuudet ulkoisista palvelutoimittajista.
Lisätiedot	– kriittisten palveluiden toimittajat ja niiden häiriöiden vaikutukset organisaation toimintaan

---

Väittämän nro	**74**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaation kriittisiin palveluihin liittyviä riskejä arvioidaan ja hallitaan säännöllisesti ja kattavasti yhteistyössä palvelutoimittajien kanssa.
Lisätiedot	– kuvattu menettely ja näyttöä sen toimivuudesta

Väittämän nro	**75**

Osa-alue	**Kyberturvallisuus**
Kuvaus	Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa.
Lisätiedot	– kuvattu menettely ja näyttöä sen toimivuudesta

Väittämän nro	**76**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatio on varautunut ja laatinut suunnitelman siihen kohdistuvan mustamaalaus- tai vaikuttamiskampanjan varalta.
Lisätiedot	– toimintatavat kuvattu

Väittämän nro	**77**
Osa-alue	**Kyberturvallisuus**
Kuvaus	Organisaatiolla on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta organisaation toimintaan.
Lisätiedot	– toimintatavat kuvattu