Porin kaupunginhallitus

Lausunto tiedonhallintalautakunnan suosituksesta julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä

Tiedonhallintalautakunnan tietoturvallisuusjaosto on pyytänyt kommentteja ja huomioita julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä laadittavana olevaan suositukseen. Kommenttipyynnössä pyydetään kiinnittämään huomiota ohjeistuksen ymmärrettävyyteen, käyttötapausten tarkoituksenmukaisuuteen sekä laaditun työkalun toimivuuteen. ICT-yksikön vt. päällikkö Ilkka Manninen ja hallintopalveluiden yksikön päällikkö Maija Hiihto ovat laatineet asiassa alla olevan lausunnon kaupunginlakimiehen lausuntopyynnön johdosta.

Julkri-suositus

Tiedonhallintalailla pyritään yhdenmukaiseen, laadukkaaseen ja tietoturvalliseen tietoaineistojen käsittelyyn julkishallinnossa. Julkri-suosituksen sivulla 6 todetaan suosituksen tarkoituksesta ja hyödyistä, että kriteeristön käyttö tukee organisaatioita tietoturvallisuuden ja henkilötietojen suojaamisen suunnittelussa, toteuttamisessa ja arvioinnissa. Ja edelleen, että ”organisaatio voi käyttää Julkria toimittajan arvioinnissa tavoitteenaan tunnistaa vaatimukset toimittajalle kilpailutuksessa tai osana palvelusopimusta sekä varmistaa vaatimusten toteutuminen toimittajan toiminnassa.”

Julkri-suositus on jaettu viiteen eri osa-alueeseen: Hallinnolliseen, fyysiseen ja tekniseen turvallisuuteen, varautumiseen ja jatkuvuudenhallintaan sekä tietosuojaan. Hallinnollisen turvallisuuden osalta (Julkri-suositus, s. 8-9) todetaan, että osa-alue kattaa yleisen hallinnollisen turvallisuuden, henkilöstöturvallisuuden sekä tietojärjestelmien ja niiden hankinnan sekä käyttöturvallisuuden kriteereitä. Kriteeristö on laaja, mutta sen piiriä voisi laajentaa vielä hallinnollisen kriteeristön kohdassa HAL – 16.1 käsiteltyjen hankintojen turvallisuuden sekä järjestelmätoimittajien kanssa laadittavien sopimusten haasteiden osalta.

Kriteeristö -Liite 1 A ja B

Yleiset kommentit kriteereistä

Julkiselle hallinnolle laaditut tietoturvallisuuden arviointikriteerit ovat tarpeen viranomaisten tietovarantojen yhdenmukaisen, laadukkaan ja tietoturvallisen hallinnan ja käsittelyn edistämiseksi tiedonhallintalain tavoitteiden saavuttamiseksi.

Julkri-kriteeristö on laaja ja kattava ja tietosuoja on kirjattuna siihen omana erillisenä kokonaisuutenaan. Myös kriteeristön taso vaikuttaa toimivalta.

Kommentit hallinnollisen turvallisuuden osa-alueeseen
Hallinnollisen turvallisuuden osalta kriteeristöön voisi lisätä järjestelmätoimittajien sopimuksiin liittyviä kriteereitä järjestelmätoimittajien omistajavaihdosten osalta. Omistajanvaihdos saattaa aiheuttaa riskin jatkuvuudenhallinnalle. Lisäksi järjestelmän omistuksen siirtyminen esimerkiksi ulkovaltojen tiedustelupalveluja lähellä oleville tahoilla voi johtaa salaisen aineiston vuotamiseen.
Kohdassa HAL-16.1 ”Hankintojen turvallisuus - sopimukset” alakohtaan ”Yleiskuvaus” voisi lisätä, että muuttuvat turvallisuusuhat edellyttävät ennakolta varautumista sopimusehdoissa. Organisaation riskit tulisi rajata sopimusehdoin järjestelmien omistajanvaihdostilanteissa.

Kommentit fyysisen ja teknisen turvallisuuden, varautumisen ja jatkuvuuden hallinnan sekä tietosuojan osa-alueisiin
Kriteeristö esittää hyvin jäsenneltyinä ja esimerkkien avustuksella myös havainnollisesti fyysisen ja teknisen turvallisuuden, varautumisen ja jatkuvuuden hallinnan sekä tietosuojalainsäädännön vaatimukset.

Kommentit Julkri työkaluun ja ohjeeseen (Liite 2 ja 3)
Julkri-työkalu
Yhdenmukainen tietoaineistojen käsittely edellyttää ohjausta, mihin Julkri-työkalu hyvin vastaa.
Julkri-työkalun ohjeistus
Yhdenmukainen tietoaineistojen käsittely edellyttää ohjausta, mihin Julkri-työkalu hyvin vastaa.

Muita kommentteja ja kehitysideoita
Suosituksen käyttöönottamista edistäisi toimijoiden yhteiset sivustot hyvien käytänteiden käyttöönottamiseksi ja hallitsemiseksi.