

Tietohallinto

28.3.2025

## **Pohteen tietoturva vaatimusten ja tietoturvaliitteen tulkintaohje hankinnoissa**

Pohde käyttää ICMT-hankinnoissaan tietoturvan osalta vakiomuotoisia vaatimusliitteitä. Liitteet ovat perustason tietoturva vaatimukset, korotetun tason tietoturva vaatimukset ja tietoturvaliite.

Pohde määrittää hankintakohtaisesti käyttääkö se perustason tietoturva vaatimuksia vai korotetun tason tietoturva vaatimuksia. Tietoturva vaatimukset kohdistuvat ensisijaisesti hankinnan kohteeseen. Tietoturvasuusliitteellä sovitaan toimittajan ja tilaajan välisistä tietoturvasuuteen liittyvistä seikoista, sekä hankinnan kohteen ylläpitoon liittyvistä tietoturvasuusperiaatteista.

Pohteen perustason- ja korotetun tason tietoturva vaatimukset ovat kyberturvasuusalan yleisten hyvien käytäntöjen mukaisia ja laadittu siten, että tarjoajalla/toimittajalla on mahdollisuus soveltaa vaatimuksia parhaaksi katsomallaan tavalla. Vaatimusten ei haluta rajoittavan teknologisia ratkaisuja, mutta kuitenkin varmistavan, että tietoturvan osalta oleelliset seikat toteutuvat.

Tietoturva vaatimukseen ei ole kuvattu tarkkoja esimerkkejä vaatimuksien soveltamisesta, koska samoja vaatimuksia käytetään erilaisiin ICMT-hankintoihin ja voi johtaa siihen, että esimerkit rajoittavat tai ohjaavat tarjoajan/toimittajan teknologisia ratkaisuja.

Mikäli Pohteen tietoturva vaatimuksissa olevan ohjeistuksen mukaisesti toimittaja ei pysty täyttämään asetettua vaatimusta, tai sitä ei voida soveltaa kyseisessä hankinnassa, on toimittajan tehtävä selvitys kunkin vaatimuksen osalta sarakkeeseen D. Tilaaja arvioi selvitykset ja hyväksyy tai hylkää ne. Tarvittaessa tilaaja pyytää tarkennuksia toimittajalta/tarjoajalta, jotta mahdollinen tarjouspyynnön jättäminen ei esty yksipuolisen tulkinnan mukaan.

Tarjoajan/toimittajan ilmoitettava ja perusteltava mikäli katsoo, että jotakin vaatimusta ei voida soveltaa tarjoajan/toimittajan ratkaisuun. Pohde tulkitsee, että toimittaja pystyy vaatimukset täyttämään, mikäli sarake D jätetään tyhjäksi, tai tarjoaja/toimittaja ei muilla keinoin viesti hankintaprosessin aikana vaatimukseen liittyvistä seikoista.